MICROCOPY RESOLUTION TEST CHART

AD A098441

FOREIGN TECHNOLOGY DIVISION

MACHINE ARITHMETIC IN RESIDUAL CLASSES

by

I. Ya. Akushshkiy, D. I. Yuditskiy

DTIC
SELECTED
MAY 0 4 1981
E

DTIC FILE COPY

81 5 01 046

UNEDITED MACHINE TRANSLATION

FTD-ID(RS)T-0239-81   3 Apr 1981

MICROFICHE NR: FTD-81-C-000293L

MACHINE ARITHMETIC IN RESIDUAL CLASSES

By: I. Ya. Akushskiy, D. I. Yuditskiy

English pages: 717

Mashinnaya Arifmetika v Ostatochnykh
Klassakh, Publishing House "Sovetskoye
Radio", Moscow, 1968 pp. 1-439.

Country of origin: USSR
This document is a machine translation
Requester: FTD/SD
Aproved for public release; distribution
unlimited.

TABLE OF CONTENTS

1

U. S. BOARD ON GEOGRAPHIC NAMES TRANSLITERATION SYSTEM

Block	Italic	Transliteration	Block	Italic	Transliteration
А а	*А а*	A, a	Р р	*Р р*	R, r
Б б	*Б б*	B, b	С с	*С с*	S, s
В в	*В в*	V, v	Т т	*Т т*	T, t
Г г	*Г г*	G, g	У у	*У у*	U, u
Д д	*Д д*	D, d	Ф ф	*Ф ф*	F, f
Е е	*Е е*	Ye, ye; E, e*	Х х	*Х х*	Kh, kh
Ж ж	*Ж ж*	Zh, zh	Ц ц	*Ц ц*	Ts, ts
З з	*З з*	Z, z	Ч ч	*Ч ч*	Ch, ch
И и	*И и*	I, i	Ш ш	*Ш ш*	Sh, sh
Й й	*Й й*	Y, y	Щ щ	*Щ щ*	Shch, shch
К к	*К к*	K, k	Ъ ъ	*Ъ ъ*	"
Л л	*Л л*	L, l	Ы ы	*Ы ы*	Y, y
М м	*М м*	M, m	Ь ь	*Ь ь*	'
Н н	*Н н*	N, n	Э э	*Э э*	E, e
О о	*О о*	O, o	Ю ю	*Ю ю*	Yu, yu
П п	*П п*	P, p	Я я	*Я я*	Ya, ya

*ye initially, after vowels, and after ъ, ь; e elsewhere.
When written as ë in Russian, transliterate as yë or ë.

RUSSIAN AND ENGLISH TRIGONOMETRIC FUNCTIONS

Russian	English	Russian	English	Russian	English
sin	sin	sh	sinh	arc sh	sinh‾
cos	cos	ch	cosh	arc ch	cosh‾
tg	tan	th	tanh	arc th	tanh‾
ctg	cot	cth	coth	arc cth	coth‾
sec	sec	sch	sech	arc sch	sech‾
cosec	csc	csch	csch	arc csch	csch‾

Russian	English
rot	curl
lg	log

MACHINE ARITHMETIC IN RESIDUAL CLASSES.

I. Ya. Akushskiy, D. I. Yuditskiy.

TRANSLATOR'S NOTE: The word Dale should read dividing.

Page 2.

The book is the original monograph, which contains the results of research of the authors on the development of arithmetic systems in the residual classes and their realizations in computer technology. By the authors are stated the bases of the new numeration system and is constructed machine arithmetic in this system. System in the residual classes ascending by its ideological roots to the classical sections of the theory of numbers, makes it possible in a new way to approach the construction of the computers of high efficiency. In the book are stated the bases of the special self-correcting nonpositional code systems.

And to the basis of the theory complex ones by integers in the field of whole real numbers without the distribution into the real and alleged parts.

The book is intended for engineers, scientific workers and students of the senior courses, which specialize in the area of computational technology.

44 Tables, 51 illustration, 79 titles bibliography.

Page 3.

PREFACE.

The results carried out during the last few years by different ones to the groups of the researchers of the searches for the ways of increasing the productivity of electronic computers, methods of organizing the efficient acquisition system and correction of errors and building of highly reliable computer complexes predicated the authors in the opinion that in the limits of the positional numeration systems it is not possible to expect any satisfactory advance in these directions without a considerable increase in the operating frequencies of elements/cells and complication of the equipment part of digital computer.

As jerk/impulse to the research in the field of the nonpositional numeration systems were used the published in 1955-1957 work of Czech scientists M. Valakh and A. Svoboda, dedicated to the representation of numbers in the form of the set of non-negative deductions of the group of mutually simple bases/bases, and determined in connection with this representation possibility of executing the rational operations without taking into account the

discharging connections between the digits of a number.

The carried out by the authors this books investigations in this new numeration system, named the system of residual classes, led to the creation of very peculiar machine arithmetic.

The difficulties of execution in the system of the residual classes of the operations, requiring knowledge of entire number as a whole, but its not single step-by-step digits (determination of the sign of a number, the comparison of numbers in the value, division in general and the like), proved to be not insurmountable. Came to light the possibilities of eliminating these difficulties by different ones in their content and character of realization by methods.

Page 4.

In the process of research of specific character and possibilities of the system of residual classes it was possible to construct the self-correcting codes, completely arithmetic, i.e., suitable for detection and correction of the errors, which appear not only during the transmission of information, but also during its arithmetic processing. For these codes it proved to be possible (which, until now, was observed not in what known special positional code systems) to construct the system of the correction of errors

during the introduction to minimum redundancy, the using dynamics of computational process.

It was explained also that the idea of residual classes makes it possible in a new way to approach the organization of analog computers. Were planned the ways of the construction of continuous type devices/equipment, which make it possible to increase substantially the accuracy of the solution on these devices/equipment of tasks with the relatively low precision of quite analog equipment.

The system of residual classes makes it possible to substantially improve the parameters of computers in comparison with the machines, constructed on the same physicotechnological basis, but in the positional numeration system, and to also obtain new more progressive constructive and structural solutions.

It should be noted that the system of residual classes not the only possible nonpositional numeration system. It is possible to construct the series/row of the new systems, to different degree which combine the special features/peculiarities of the positional and nonpositional numeration systems. However, the results of research according to the general theory of nonpositional systems are not connected with the present monograph, taking into account its thematic directionality.

The ideas of the nonpositional numeration systems do not draw
thus far so wide a contingent of scientific and engineering workers,
as these ideas of that deserve. This worthy of regret circumstance is
explained by the mainly fact that the results of the majority of
research in the region of nonpositional systems yet did not become
the property of the wide circle of the specialists in view of the
absence of the properly systematized publications. Literature in this
series of question consists only of the small series of article and
furthermore of those published in the little encountered
publications.

Specifically, the intention to complete this gap/spacing led by
the authors, who launched in this monograph the attempt to
systematically present the basic theoretical and practical aspects of
the system of residual classes.

Page 5.

For the purpose of simplifying to reader the mastery/adoption of
the material of the book is introduced chapter 2, in which is
presented the necessary information from the theory of numbers, it is
more exact, comparisons. For this purpose the almost each paragraph

of the book is accompanied by the illustrating the set-forth positions examples.

Besides chapter 2 and partially chapter 1 monograph, in essence contains the presentation of the original research, carried out by the authors in the latter/last decade.

Unfortunately, the series/row of important and useful sections they could not be connected with the book in view of the limitedness of its capacity. In reader's this plan/layout after acquaintance with the material, presented in this book, it is necessary to refer to to some special articles.

The book is intended for the scientific workers and engineers, who carry out the development of electronic computers, and the students of the senior policies of higher educational institutions for the appropriate specialties.

The authors express hope, that the appearance of this book will contribute to the expansion of research according to the theory and to the practical realization of numeration system in the residual classes and to the introduction of this system into computer technology.

                                                              Authors.

Page 6.

No typing.

Page 7.

Chapter 1.

INTRODUCTION TO NUMERATION SYSTEM IN THE RESIDUAL CLASSES.

§1.1. Emergence and the development of the nonpositional numeration systems.

At present it is not possible to visualize any complicated automatic system without its center section being composed of the computers, which fulfill the functions of processing information and control. Actually, in each automatic system specific are the sensors of information and actuating elements, and in other respects system often consists of the standard computers, which ensure interconnection and coordinated interaction of all devices/equipment of system.

Therefore is obvious the value of the research, dedicated to the new principles of the construction of electronic computers, to the rational methods of organizing their work, to the searches for effective means of their use/application.

The new ways of organizing of structure and logic of electronic computers encompass both the directions of the complication of structure and logic of machines for an increase in their efficiency and search for the new systems of numeration and new methods of organizing the joint operation of all devices/equipment of machine and entire machine as a whole.

Page 8.

During the development of the structure of mathematical machine one of the basic questions is the selection of the appropriate representation of numerical information, i.e., the corresponding code. Numeration systems are the different methods of the coding of numerical information.

Principal requirements for any intended for the practical use/application code system (if we clear the requirements, which escape/ensue from the information theory considerations) essence following:

a) the possibility of representation in this system of any value in the considered/examined, predetermined range;

b) the uniqueness of representation - any code combination

corresponds to one and only to one number in the preset range;

c) simplicity of operation with numbers in this numeration system.

The capacity of range, i.e., a quantity of different numbers which can be represented in this code system, obviously, is determined by the number of different possible code combinations.

The searches for the new ways of increasing the efficiency in the execution of arithmetic operations led researchers to the conclusion that within the framework of the ordinary positional system of the considerable acceleration of the execution of operations cannot be attained almost. These or other single methods and improvements of the algorithms of the execution of operation, contributing to the more rational organization of work of arithmetic units, leave nevertheless the productivity of these devices/equipment within the framework of one and of the same order. Output/yield beyond these limits requires the enlistment of new ideas, new logic and new arithmetic.

It should be noted that the positional systems of the numerations, in which is represented and is treated the information in the contemporary computers, possess essential deficiency/lack -

the presence of the interbit/interbyte connections which superimpose
their print on the methods of the realization of arithmetic
operations, complicate equipment and limit high speed. Therefore is
logical the research of the possibilities of the construction of such
arithmetic, in which step-by-step connections were absent.

It turned out that this arithmetic can be constructed on the
basis of the nonpositional system of numeration, in particular
numeration systems in the residual classes.

Page 9.

Ascending by its ideological roots to the classical works of
Euler, Gauss and Chebyshev according to the theory of comparisons the
system of residual classes is intended to introduce new jet into the
development of the principles of the efficient construction of
high-productivity computers.

In the system of residual classes numbers are represented by
their remainders/residues from the division into the selected system
of bases/bases, and all rational operations can be made in parallel
above the digits of each digit individually. However, in so
convenient a in one sense system of residual classes is inherent the
number of deficiencies/lacks in other respects: the limitedness of

the operation of this system by the field positive integer numbers,
the difficulty of determining the relationships/ratios of numbers
from the value, the determination of the output/yield of result of
operation from the range, etc.

So that in the system of residual classes it would be possible
to construct computers, it is necessary to find the fundamental ways
of overcoming these difficulties and to find the efficient methods of
the construction of machine arithmetic.

§1.2. Positional numeration systems the formation/education of the
digits of the representation of a number.

Determination. If is preset the series/row positive integer
numbers $\pi_1, \pi_2, \ldots, \pi_n$, subsequently of those called rice, then under
the generalized positional system we will understand such system, in
which integer N is represented in the form

$$N = a_{n-1}\pi_{n-1}\pi_{n-2} \ldots \pi_2\pi_1 + a_{n-2}\pi_{n-2}\pi_{n-3} \ldots \pi_2\pi_1 + \ldots$$
$$\ldots + a_2\pi_2\pi_1 + a_1\pi_1 + a_0. \qquad (1.1)$$

where digit a_{j-1} are numbers $0, 1, \ldots, \pi_j - 1 \ (j = 1, 2, \ldots, n)$, consecutive
obtaining of which can be realized by the following process:

$$N \overset{(1)}{\text{делится на}} \pi_1, \overset{(2)}{\text{при этом}} \left[\frac{N}{\pi_1}\right] = N_1 \text{ и } N - N_1\pi_1 = a_0;$$

$$N_1 \overset{(3)}{\text{делится на}} \pi_2, \overset{(4)}{\text{при этом}} \left[\frac{N_1}{\pi_2}\right] = N_2 \text{ и } N_1 - N_2\pi_2 = a_1;$$

$$N_{j-1} \overset{(5)}{\text{делится на}} \pi_j, \overset{(6)}{\text{при этом}} \left[\frac{N_{j-1}}{\pi_j}\right] = N_j \text{ и } N_{j-1} - N_j\pi_j = a_{j-1};$$

$$N_{n-1} \overset{(7)}{\text{делится на}} \pi_n, \overset{(8)}{\text{при этом}} \left[\frac{N_{n-1}}{\pi_n}\right] = N_n \text{ и } N_{n-1} - N_n\pi_n = a_{n-1}.$$

Key: (1). it is divided into. (2). in this case.

Page 10.

Here and subsequently [Y] it designates whole syllable Y.

The capacity of the range of represented in this system numbers $\mathcal{P}$ is equal to

$$\mathcal{P} = \pi_1\pi_2 \ldots \pi_n.$$

For the described process characteristically precisely consecutive obtaining of the digits of each digit in the strictly defined order (beginning from the low-order digit), when the result of the previous stage (obtained in this stage quotient) participates as the dividend in the following stage. This reflects the inherent in the positional numeration systems dependence between the digits of a number, which with the fulfillment of the operations on numbers in the positional system imply the need for the account of transfers from the low-order digits into the adjacent senior. This dependance

of digits burdens to a considerable degree the equipment execution of operations and limits possibilities in the achievement of high speed operation and simplicity of realization.

If we introduce the designation

$$p_i = \pi_1 \pi_2 \ldots \pi_i,$$

the expression (1.1) can be registered in the form

$$N = a_{n-1}p_{n-1} + a_{n-2}p_{n-2} + \ldots + a_1 p_1 + a_0. \qquad (1.2)$$

In the particular case $\pi_1 = \pi_2 = \ldots = \pi_n = p$ we will obtain

$$N = a_{n-1}p^{n-1} + a_{n-2}p^{n-2} + \ldots + a_1 p + a_0. \qquad (1.3)$$

Here all consecutive indexings are conducted on one and the same number p - base of system, and we thus obtained the ordinary positional system, whose capacity $\mathscr{P}$ of the range of represented in this system numbers was equal to

$$\mathscr{P} = p^n.$$

Choosing basis/base p equal to 2, 3 ..., it is possible to sort out all possible positional numeration systems.

In the digital electronic computers prevailing value obtained binary and decimal systems. The latter larger partly is applied in the binary-coded form. Are known machines, constructed in the ternary system, numeration system with basis/base $p = -2$, etc.

Page 11.

The advisability of the introduction of negative bases/bases depends
on the fact that the sign organically is included in the
representation of a number, in connection with which there is no need
for in the special representation of the sign of a number.

Inconveniance in the realization of this system consists in the
process of addition - to one digit can arrive two transfers, which
complicates the diagram of adder .

From the point of view of the range of the represented numbers
in the case of negative basis/base occurs certain dissymmetry. Thus,
with even n (or with an even quantity of digits of a number) of the
negative numbers it can be represented more than positive ones, and
with the odd vice versa.

For example, with n=4 entire/all set of numbers is such:

$$
\begin{array}{lll}
0001 = +1 & 0110 = +2 & 1011 = -9 \\
0010 = -2 & 0111 = +3 & 1100 = -4 \\
0011 = -1 & 1000 = -8 & 1101 = -3 \\
0100 = +4 & 1001 = -7 & 1110 = -6 \\
0101 = +5 & 1010 = -10 & 1111 = -5.
\end{array}
$$

Here positive numbers 1, 2, 3, 4, 5, and negative 1, 2, 3, 4, 5, 6,
7, 8, 9, 10, i.e. the range of negative numbers are twice more than

as the range of positive numbers.

For case of n=3 the set of the represented numbers will be
registered in the form

$$001 = +1 \qquad 101 = +5$$
$$010 = -2 \qquad 110 = +2$$
$$011 = -1 \qquad 111 = +3$$
$$100 = +4$$

In this case the range of positive numbers more than twice
exceeds the range of negative ores.

Are known the reflected in large quantities of works different
logical and circuit methods of acceleration and rational organization
of the execution of operations.

Page 12.

In all these works as basis was assumed positional system, and one
should, apparently, consider that proposed in these works ways of the
more efficient execution of operations exhaust in many respects of
possibility the positional of system and further any considerable
acceleration of the execution of operations, remaining within the
framework of positional system, is hindered/hampered.

The searches for the new ways of the construction of the

arithmetic units, in which the operations on numbers would be made as
simply as possible, moreover so, that the dependence between bits was
excluded and would drop out interbit/interbyte transfers, they led to
the use/application for these purposes of the apparatus of calculus
of residues. The deductions have been known for a long time   and are
stated in the elementary course of the theory of numbers; however,
until recently the possibility of their practical use in computer
technology was not examined.

The theory of numbers applies deductions for solving the
series/row of specific for this field of science tasks (comparison,
diophantine analysis, etc.). Meanwhile the use/application of
deductions as the nonpositional numeration system in computer
technology places other entirely problems, on successful solution of
which depends not only the efficiency, but also generally the
advisability of applying this system.

1.3. Numeration system in the residual classes.

Determination. If is preset the series/row of positive integers
$p_1, p_2, \ldots, p_n$, of those called subsequently the basis of system, then
under numeration system in the residual classes we will understand
such system, in which positive integer number is represented in the
form of the set of remainders/residues (deductions) on the selected

bases/bases

$$N = (\alpha_1, \alpha_2, \ldots, \alpha_n).$$

moreover the formation/education of digits α_i is realized by the following process

$$\alpha_i = N - \left[\frac{N}{p_i}\right] p_i \text{ for } i = 1, 2 \ldots n, \qquad (1.4)$$

i.e. the digit of i digit α_i of number N e the smallest positive remainder/residue from division of N on p_i.

Here in contrast to the generalized positional system formation of the digit of each bit will foresee itself independently of each other. The digit of i digit α_i is the smallest positive remainder/residue from the division of very number N, but the not previous quotient, as this occurred into §1.2, to i basis/base π_i. It is obvious that $\alpha_i < p_i$.

Page 13.

In the theory of numbers it is proved that if numbers p_i are the mutually simple between themselves, then the described by digits $\alpha_1, \alpha_2, \ldots, \alpha_n$ representation of number N is single.

The capacity of the range of the represented numbers in this case, as can easily be seen, is equal to

$$\mathscr{P} = p_1 p_2 \ldots p_n.$$

Here, as in the generalized positional system, the range of the represented numbers he increases as the product of bases/bases, and the bit configuration of numbers N he increases as the sum of the bit configurations of the same bases/bases.

Let us consider the rules of the execution of the operations of addition and multiplication in the system of residual classes if both numbers and result of operation are found in the range $(0, \mathscr{P})$. Let operands A and B be represented respectively by remainders/residues α_i and β_i on bases/bases p_i with $i = 1, 2, \ldots, n$.

The results of operation of addition and multiplication A+B and AB are represented respectively by remainders/residues γ_i and δ_i on the same bases/bases p_i, i.e.

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n),$$
$$B = (\beta_1, \beta_2, \ldots, \beta_n),$$
$$A + B = (\gamma_1, \gamma_2, \ldots, \gamma_n),$$
$$AB = (\delta_1, \delta_2, \ldots, \delta_n).$$

and in this case occur the relationships/ratios:

$$A < \mathscr{P}, \; B < \mathscr{P}, \; A+B < \mathscr{P}, \; AB < \mathscr{P}.$$

It is claimed that γ_i is congruent with $\alpha_i + \beta_i$ in modulus/module p_i. and δ_i is congruent with $\alpha_i \beta_i$ in the same modulus/module, i.e.,

$$\gamma_i \equiv \alpha_i + \beta_i \pmod{p_i},$$
$$\delta_i \equiv \alpha_i \beta_i \pmod{p_i},$$

In this case as the digit of result it is taken respectively

$$\gamma_i = \alpha_i + \beta_i - \left[\frac{\alpha_i + \beta_i}{p_i}\right] p_i, \qquad (1.5)$$

$$\delta_i = \alpha_i \beta_i - \left[\frac{\alpha_i \beta_i}{p_i}\right] p_i. \qquad (1.6)$$

Actually/really, on the basis (1.4) it is possible to write

$$\gamma_i = A - B - \left[\frac{A - B}{p_i}\right] p_i$$
$$\text{(1)}$$
$$\text{для } i = 1, 2, \ldots, n.$$

Key: (1). for.

Page 14.

From representation A and B it follows that

$$A = k_i p_i + \alpha_i; \qquad (1.7)$$
$$B = l_i p_i + \beta_i,$$
$$i = 1, 2, \ldots, n,$$

where k_i and l_i - whole non-negative numbers. Then

$$A + B = (k_i + l_i) p_i + \alpha_i + \beta_i,$$
$$\left[\frac{A + B}{p_i}\right] = k_i + l_i + \left[\frac{\alpha_i + \beta_i}{p_i}\right],$$
$$i = 1, 2, \ldots, n$$

whence

$$\gamma_i = \alpha_i + \beta_i - \left[\frac{\alpha_i + \beta_i}{p_i}\right] p_i,$$

that also proves (1.5).

In the case of the multiplication

$$\delta_i = AB - \left[\frac{AB}{p_i}\right] p_i.$$

Taking into account (1.7), we will obtain

$$AB = k_i l_i p_i^2 + (\alpha_i l_i + \beta_i k_i) p_i + \alpha_i \beta_i,$$
$$\left[\frac{AB}{p_i}\right] = k_i l_i p_i + \alpha_i l_i + \beta_i k_i + \left[\frac{\alpha_i \beta_i}{p_i}\right],$$
$$i = 1, 2, \ldots, n.$$

Consequently,

$$\delta_i = \alpha_i \beta_i - \left[\frac{\alpha_i \beta_i}{p_i}\right] p_i,$$

that also proves (1.6).

Let us consider the examples, which illustrate the given above rules of the execution of the operations of addition and multiplication.

Let the basis of system be

$$p_1 = 3, \quad p_2 = 5, \quad p_3 = 7.$$

The range of system will be defined as $\mathscr{P} = p_1 p_2 p_3 = 105$.

Example. To sum number A=17 with number B=63.

On the selected bases/bases numbers A and B in the system of residual classes will be represented as

$$A = 17 = (2, 2, 3),$$
$$B = 63 = (0, 3, 0).$$

In accordance with (1.5) we will obtain

$$A + B = (2, 0, 3).$$

Page 15.

Easily it is checked, that number (2, 0, 3) is 80 equal to the sum of operands.

Example. To multiply number A=17 by number B=6.

In the system of residual classes numbers A and B will be represented as

$$A = 17 = (2, 2, 3),$$
$$B = 6 = (0, 1, 6).$$

In accordance with (1.6) we will obtain

$$AB = (0, 2, 4).$$

Easily it is checked, that number (0, 2, 4) is 102 and it is equal to the product of operands.

Let us describe in general terms the advantages and disadvantages in the introduced numeration system in the residual classes.

To the advantages should be related:

- the independence of the formation/education of the bits of a number, by virtue of which each bit carries information about entire initial number, but not about the intermediate number, which is

obtained as a result of forming the low-order bits (as it takes place in the positional system). Hence ensues/escapes/flows out the independence of the bits of a number from each other and the possibility of their independent parallel processing [1];

- Low-nature of the remainders/residues, which represent a number.

FOOTNOTE [1]. This special feature/peculiarity subsequently will make it possible to draw fundamentally new methods of arithmetic check. During the introduction of further control basis/base the remainder/residue, undertaken on this basis/base, carries surplus information about an initial number, which makes it possible to discover and to correct the errors in the digits from the working basis of system. ENDFOOTNOTE.

In view of the small number of possible code combinations is disclosed the possibility of the construction of tabular arithmetic, thanks to which the majority of the operations, performed by arithmetic unit, are converted into the single-cycle ones, implemented by simple sample of the table.

Page 16.

To main disadvantages in the numeration system in the residual classes should be related:

- the impossibility cf the visual comparison of numbers, since the external recording cf a number does not give representaticn about its value;

- absence of the simple signs/criteria of the output/yield of results cf cperaticn beycnd the limits of range $(0, \mathscr{F})$;

- the limitedness cf the cperation of system by the sphere positive integer numbers;

- obtaining in all cases of accurate result of operation, which excludes the possibility cf the direct approximate executicn cf operations, rounding of result, etc.

The elimination of deficiencies/lacks in the system or at least weakening the operaticn cf these deficiencies/lacks and most complete use of its advantages in the implementation in the computers compose the basic content of machine arithmetic in the system of residual classes creation by which puts forth its specific problems.

§1.4. Methods of the intrcducticn of negative numbers.

The given above representations of numbers and operations above them related to the positive numbers.

Let us consider the rules of the execution of the operation of subtraction in the system of residual classes if both numbers and result of operation are found in the range $[0, \mathscr{P}]$.

Let operands A and B be represented respectively by remainders/residues α_i and β_i on bases/bases p_i with i=1, 2, ..., n. The result of operation of subtraction A-B is represented respectively by remainders/residues γ_i on the same bases/bases p_i. i.e.

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$$
$$B = (\beta_1, \beta_2, \ldots, \beta_n).$$
$$A - B = (\gamma_1, \gamma_2, \ldots, \gamma_n),$$

and in this case occur relationships/ratios: $A < \mathscr{P}$, $B < \mathscr{P}$, $0 \leqslant A - B < \mathscr{P}$. Analogous (with 1.5) we will obtain for the subtraction

$$\gamma_i = \alpha_i - \beta_i - \left[\frac{\alpha_i - \beta_i}{p_i} \right] p_i. \qquad (1.8)$$
$$\gamma_i \equiv \alpha_i - \beta_i \ (\mathrm{mod}\ p_i).$$
$$i = 1, 2, \ldots, n.$$

The operation of subtraction when its result is positive, is implemented by the subtraction of the corresponding digits of digits,

moreover as a result is always given the smallest positive remainder/residue, as this follows from the determination of the system of residual classes.

In other words if a difference in the digits proved to be negative, then is taken its addition to the basis/base.

Page 17.

After the execution of operation the sign of result in any way in it in is reflected. Strictly speaking the signs of components with the execution of operation are not treated and, therefore, is not formed the sign of result.

Appears the need for introducing in a special manner sign into the representation of a number and determining the rules of the execution of operation, which ensure obtaining not only the value of result, but also its sign.

Let us consider the possible versions of the introduction of negative numbers.

$p_1, p_2, \ldots, p_n$ - radix. Range $\mathcal{P}$ of represented in this system numbers will be defined as

$$\mathcal{P} = p_1, p_2, \ldots, p_n.$$

Let one of the basis of system be equal to 2. For the certainty we assume/set $p_1 = 2$.

Let us designate through P value

$$P = \frac{\mathcal{P}}{p_1} = \frac{1}{2}\mathcal{P}$$

or

$$P = p_2 p_3 \ldots p_n.$$

In the system of the residual classes

$$P = (1, 0, 0, \ldots, 0).$$

We will use with the numbers, which lie in the range,

$$0 \leqslant |N| < P.$$

Let us take as zero numbers P and we will represent positive numbers $N = |N|$ in the form $N' = P + |N|$, and negative numbers $N = -|N|$ in the form $N' = P - |N|$. Then with the algebraic addition we obtain the following form of the representation of the positive and negative numbers:

$$N' = P + N.$$

This means that in the representation accepted which let us name artificial form, we will always deal concerning the positive numbers. However numbers in the interval [0, P) in the artificial form there will represent negative numbers, and in interval $(P, \mathcal{P})$ - positive.

Page 18.

If result of operation does not exceed the limits of new range [0, P), it is possible to implement the operations of addition and subtraction as follows.

Assume it is necessary to find the sum of two numbers N_1 and N_2. Let us take their artificial forms

$$N_1' = P + N_1, \quad N_2' = P + N_2$$

and let us sum

$$N_1' + N_2' = P + N_1 + P + N_2 = 2P + (N_1 + N_2). \quad (1.9)$$

The artificial form of sum is

$$(N_1 + N_2)' = (N_1 + N_2) + P, \quad (1.10)$$

whence

$$(N_1 + N_2)' = N_1' + N_2' - P,$$

or, the same, since P= (1, 0, 0, ... 0),

$$(N_1 + N_2)' = N_1' + N_2' + P. \quad (1.11)$$

Let us consider the examples, which illustrate the formulated rules. In these examples it is assumed:

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \quad P = 3 \cdot 5 \cdot 7 = 105.$$

Example. $N_1 = 17$, $N_2 = 41$. We form the artificial forms of the preset numbers

$$N_1' = (1, 0, 0, 0) + (1, 2, 2, 3) = (0, 2, 2, 3),$$
$$N_2' = (1, 0, 0, 0) + (1, 2, 1, 6) = (0, 2, 1, 6),$$

on the basis (1.11) obtain

$$(N_1 + N_2)' = (0, 2, 2, 3) + (0, 2, 1, 6) + (1, 0, 0, 0) = (1, 1, 3, 2).$$

Number (1, 1, 3, 2) is the artificial form of the sum of the preset numbers, what is checked by transition to the decimal system:

$$(17+41)' = (58)' = 105 + 58 = (1, 0, 0, 0) + (0, 1, 3, 2) = (1, 1, 3, 2).$$

Example. $N_1 = 17$, $N_1 = -41$. We form the artificial forms of the preset numbers

$$N_1' = (1, 0, 0, 0) - (1, 2, 2, 3) = (0, 2, 2, 3),$$
$$N_2' = (1, 0, 0, 0) - (1, 2, 1, 6) = (0, 1, 4, 1).$$

Let us sum these numbers and on the basis (1.11) we will obtain

$$(N_1 + N_2)' = (0, 2, 2, 3) + (0, 1, 4, 1) + (1, 0, 0, 0) = (1, 0, 1, 4).$$

Let us produce checking by transition to the decimal system:

$$(17 - 41)' = (-24)' = 105 - 24 = (1, 0, 0, 0) - (0, 0, 4, 3) = (1, 0, 1, 4).$$

Example. $N_1 = -17$, $N_2 = -41$. We form the artificial forms of the preset numbers

$$N_1' = (1, 0, 0, 0) - (1, 2, 2, 3) = (0, 1, 3, 4).$$
$$N_2' = (1, 0, 0, 0) - (1, 2, 1, 6) = (0, 1, 4, 1).$$

Page 19.

Let us sum these numbers taking into account (1.11)

$$(N_1 + N_2)' = (0, 1, 3, 4) + (0, 1, 4, 1) + (1, 0, 0, 0) = (1, 2, 2, 5).$$

With transition to the decimal system we produce the testing

$$(-17 - 41)' = (-58)' = 105 - 58 = (1, 0, 0, 0) - (0, 1, 3, 2) = (1, 2, 2, 5).$$

The transition of positive number into the negative and back, i.e., the formation/education of its two's complement, is produced by

the subtraction of this number of the number

$$(1, p_2, p_3, \ldots, p_n).$$

Thus, under conditions of the examples examined.

$$+41 = (1, 2, 1, 6); \quad -41 = (1, 3, 5, 7) - (1, 2, 1, 6) =$$
$$= (0, 1, 4, 1) = 64.$$

It should be noted that if the subtrahend was already represented in the artificial form, then for obtaining two's complement it is necessary to subtract it not of the number $(1, p_2, \ldots, p_n)$, and from $(2, p_2, \ldots, p_n)$.

Let us consider the examples, which illustrate the method of conducting the subtraction indicated.

Example. $N_1 = 17$, $N_2 = 41$. Let us present the preset numbers in the artificial form

$$N_1' = (0, 2, 2, 3), \quad N_2' = (0, 2, 1, 6).$$

We form the two's complement N_2

$$(-N_2)' = (2, 3, 5, 7) - (0, 2, 1, 6) = (0, 1, 4, 1).$$

Let us sum N'_1 and N'_2, taking into account (1.11):

$$(N_1 - N_2)' = (N_1 + (-N_2))' = N_1' + (-N_2)' + P =$$
$$= (0, 2, 2, 3) + (0, 1, 4, 1) + (1, 0, 0, 0) = (1, 0, 1, 4).$$

On one of the previous examples it is known that $(1, 0, 1, 4) = (17-41)'$.

Example. $N_1 = 41$, $N_2 = 17$. We form the two's complement N'_2:

$(-N_2)' = (2, 3, 5, 7) - (0, 2, 2, 3) = (0, 1, 3, 4)$ and we further implement

the addition

$$(N_1 - N_2)' = N_1' + (-N_2)' + P =$$
$$= (0, 2, 1, 6) + (0, 1, 3, 4) + (1, 0, 0, 0) = (1, 0, 4, 3).$$

By transition to the decimal system we check, that

$$(41 - 17)' = (24)' = 105 + 24 = (1, 0, 0, 0) + (0, 0, 4, 3) = (1, 0, 4, 3).$$

Page 20.

From methods of procedure of addition and subtraction presented
it follows that, applying the artificial form of the representation
of the codes (with zero drift on F), is possible to carry out the
operations of addition and subtraction above the artificial forms,
obtaining always correct (both in the value, and on the sign) result,
although sign it is hidden in the form of the representation of a
number and we cannot visually determine, it is positive or negative.

Let us switch over to the operation of multiplication. As it is
above,

$$N_1' = P + N_1, \qquad N_2' = P + N_2,$$

then

$$N_1' N_2' = P(P + N_1 + N_2) + N_1 N_2, \qquad (1.12)$$

whence

$$(N_1 N_2)' = N_1' N_2' + P - P(P + N_1 + N_2).$$

Taking into account that $P = (1, 0, 0, \ldots 0)$ and that the initial
numbers are preset in the artificial form, we will obtain

$$(N_1 N_2)' = N_1' N_2' + P(1 + P + N_1' + N_2').$$

Since P is odd, we will obtain

$$(N_1 N_2)' = N_1' N_2' + P(N_1' + N_2'), \qquad (1.13)$$

It is obvious that the parity or oddness $N'_1 + N'_2$ will determine, in what form will be obtained the result.

Expression (1.13) can be registered as

$$(N_1 N_2)' = \begin{cases} N_1' N_2', & \overset{(1)}{\text{если}} N_1' \text{ и } N_2' \overset{(2)}{\text{одинаковой четности,}} \\ N_1' N_2' + P, & \overset{(1)}{\text{если}} N_1' \text{ и } N_2' \overset{(3)}{\text{разной четности.}} \end{cases} \quad (1.14)$$

Key: (1). if. (2). identical parity. (3). different parity.

One or the other alternative determines the need for the correction of result. If N'_1 and N'_2 different parity, we obtain the result of multiplication immediately in the artificial form, but if N'_1 and N'_2 of identical parity, to the result it is necessary to adjoin $P=(1, 0, \ldots, 0)$ in order to convert it into the artificial form. Since one of the basis of system was selected $p_1=2$, then in terms of the value of the remainder/residue of a number by this basis/base we judge about parity or oddness of a number itself.

Hence the analysis of a single number or sum to the parity or the oddness is produced on the single-column remainder/residue on basis/base $p_1=2$. It is logical that the odd numbers will have in the remainder/residue on this basis/base unity, and even numbers - zero.

Respectively and the correction of result, if it is required, i.e., addition P=(1, 0, 0, ..., 0), whose single remainder/residue on basis/base $p_1=2$, and others - zero, it is reduced to the inversion of the value of the remainder/residue of result on basis/base p_1.

Page 21.

Let us give the examples, which illustrate the execution of the operation of multiplication. The system of bases/bases the same as in the previous examples.

Example. $N_1=7$, $N_2=13$. Let us present the preset numbers in the artificial form

$$N_1' = (1, 0, 0, 0) + (1, 1, 2, 0) = (0, 1, 2, 0),$$
$$N_2' = (1, 0, 0, 0) + (1, 1, 3, 6) = (0, 1, 3, 6).$$

We compute product $N'_1 N'_2$:

$$N_1' N_2' = (0, 1, 2, 0) \cdot (0, 1, 3, 6) = (0, 1, 1, 0).$$

Since N'_1 and N'_2 identical parity, then

$$(N_1 N_2)' = N_1' N_2' = (0, 1, 1, 0)$$

Result we check by transition to the decimal system

$$(7 \cdot 13)' = (91)' = 105 + 91 = (1, 0, 0, 0) + (1, 1, 1, 0) = (0, 1, 1, 0).$$

Example. $N_1=7$, $N_2=-13$. Let us write artificial form for the preset numbers

$$N_1' = (1, 0, 0, 0) + (1, 1, 2, 0) = (0, 1, 2, 0),$$
$$N_2' = (1, 0, 0, 0) - (1, 1, 3, 6) = (0, 2, 2, 1).$$

Let us compute product $N'_1 N'_2$:

$$N_1'N_2' = (0, 1, 2, 0)\cdot(0, 2, 2, 1) = (0, 2, 4, 0).$$

In accordance with rule (1.14) $(N_1N_2)' = (0, 2, 4, 0)$. Checking gives the following result:

$$(7\cdot(-13))' = (-91)' = 105 - 91 = (1, 0, 0, 0) - (1, 1, 1, 0) = (0, 2, 4, 0).$$

Example. $N_1 = -7$, $N_2 = -13$. Let us present the preset numbers in the artificial form

$$N_1' = (1, 0, 0, 0) - (1, 1, 2, 0) = (0, 2, 3, 0),$$
$$N_2' = (1, 0, 0, 0) - (1, 1, 3, 6) = (0, 2, 2, 1),$$

we determine product $N'_1N'_2$:

$$N_1'N_2' = (0, 2, 3, 0)\cdot(0, 2, 2, 1) = (0, 1, 1, 0).$$

Of previously the example examined it is evident, that $(0, 1, 1, 0) = (7 \cdot 13)$ or, which is the same, $(0, 1, 1, 0) = ((-7) \cdot (-13))'$.

In the given examples were multiplied numbers of identical parity. Let us consider examples of the multiplication of numbers of different parity.

Example. $N_1 = 6$, $N_2 = 17$. Let us present the preset numbers in the artificial form

$$N_1' = (1, 0, 0, 0) - (0, 0, 1, 6) = (1, 0, 1, 6),$$
$$N_2' = (1, 0, 0, 0) - (1, 2, 2, 3) = (0, 2, 2, 3).$$

we compute product $N'_1N'_2$:

$$N_1'N_2' = (1, 0, 1, 6)(0, 2, 2, 3) = (0, 0, 2, 4).$$

Since N'_1 and N'_2 different parity, then according to (1.14)

$$(N_1N_2)' = (1, 0, 0, 0) - (0, 0, 2, 4) = (1, 0, 2, 4).$$

Page 22.

By transition to the decimal system, we check

$$(6 \cdot 17)' = (102)' = 105 + 102 = (1, 0, 0, 0) + (0, 0, 2, 4) = (1, 0, 2, 4).$$

Example. $N_1 = 6$, $N_2 = -17$.

$$N'_1 = (1, 0, 0, 0) + (0, 0, 1, 6) = (1, 0, 1, 6)$$
$$N'_2 = (1, 0, 0, 0) - (1, 2, 2, 3) = (0, 1, 3, 4)$$
$$N'_1 N'_2 = (1, 0, 1, 6) \cdot (0, 1, 3, 4) = (0, 0, 3, 3).$$

According to (1.14) we have

$$(N_1 N_2)' = (1, 0, 0, 0) + (0, 0, 3, 3) = (1, 0, 3, 3).$$

Checking by transition to the decimal system gives

$$(6 \cdot (-17))' = (-102)' = 105 - 102 = (1, 0, 0, 0) - (0, 0, 2, 4) = (1, 0, 3, 3).$$

The method presented the representations of negative numbers and operation/process with them assume that $p_1 = 2$.

This is convenient from the point of view of simplicity of the execution of operation/process, but it is certain limitation. It can seem that in the questions, connected with the approximate execution of operations/processes in the machine in the composition of the foundations for inexpediently having a basis/base, equal to two.

Therefore it is necessary to examine the process of the introduction of negative numbers of more general character, without assuming compulsorily in the composition of the bases/bases of number 2.

Let the basis of system be $p_1, p_2, \ldots, p_n$, moreover $p_1 = 2\tau + 1$. Let us break down the range $\mathcal{P} = p_1 p_2 \ldots p_n$ to two parts: $\left[0, \frac{\mathcal{P}-1}{2}\right)$ and $\left[\frac{\mathcal{P}-1}{2}, \mathcal{P}\right)$.

Let further in the adopted system number $\frac{\mathcal{P}-1}{2}$ take form $\frac{\mathcal{P}-1}{2} = (\rho_1, \rho_2, \ldots, \rho_n)$. Let us accept as zero numbers $\frac{\mathcal{P}-1}{2}$ and we will represent positive numbers $N = |N|$ in the form $N' = \frac{\mathcal{P}-1}{2} + N$, and negative numbers $N = -|N|$ in the form $N' = \frac{\mathcal{P}-1}{2} - |N|$, i.e. the general view of the artificial form of a number will be

$$N' = \frac{\mathcal{P}-1}{2} + N. \qquad (1.15)$$

The representation of a number in the form (1.15) subsequently we will call the generalized artificial form of a number.

Page 23.

Assuming that the result of operation in the absolute value does not exceed $\frac{\mathcal{P}-1}{2}$, it is possible to perform the operations/processes of addition and subtraction as follows: assume it is necessary to find the sum of two numbers N_1 and N_2, preset in the artificial form:

$$N'_1 = \frac{\mathcal{P}-1}{2} + N_1, \quad N'_2 = \frac{\mathcal{P}-1}{2} + N_2;$$

let us add these numbers

$$N'_1 + N'_2 = 2\frac{\mathcal{P}-1}{2} + N_1 + N_2.$$

The artificial form of the sum of these numbers takes the form

$$(N_1 + N_2)' = \frac{\mathcal{F}-1}{2} + N_1 + N_2.$$

Let us designate $\left(-\frac{\mathcal{P}-1}{2}\right)$ through $\frac{\overline{\mathcal{F}-1}}{2}$; $\frac{\overline{\mathcal{P}-1}}{2} = (\bar{\rho}_1, \bar{\rho}_2, \ldots, \bar{\rho}_n).$ Here $\bar{\rho}_i = p_i - \rho_i,$ i=1, 2, ..., n. Then

$$(N_1 + N_2)' = N'_1 + N'_2 + (\bar{\rho}_1, \bar{\rho}_2, \ldots, \bar{\rho}_n). \qquad (1.16)$$

It is easy to see that the two's complement of number N is obtained by the subtraction of this number of

$$\frac{\mathcal{P}-1}{2} = (\rho_1, \rho_2, \ldots, \rho_n).$$

In this case, if a number was preset in the artificial form, subtraction with the formation/education of two's complement must is carried out from

$$2\frac{\mathcal{P}-1}{2} = (p_1-1, p_2-1, \ldots, p_n-1).$$

Let us give the examples, which illustrate the addition of numbers in the artificial representation accepted. The system of base takes the form:

$$p_1 = 3, \quad p_2 = 5, \quad p_3 = 7, \quad p_4 = 11.$$

Then $\frac{\mathcal{P}-1}{2} = 577 = (1, 2, 3, 5)$ and $\frac{\overline{\mathcal{F}-1}}{2} = (2, 3, 4, 6).$

Example. $N_1 = 46$, $N_2 = 81$. Let us write the artificial forms of the components/terms/addends

$$N_1' = (1, 2, 3, 5) - (1, 1, 1, 2) = (2, 3, 0, 7)$$
$$N_2' = (1, 2, 3, 5) - (0, 1, 4, 4) = (1, 3, 0, 9).$$

Then in accordance with (1.16) we obtain

$$(N_1 + N_2)' = (2, 3, 0, 7) + (1, 3, 0, 9) + (2, 3, 4, 6) = (2, 4, 4, 0).$$

We check by transition to the decimal system, that

$$(46 + 81)' = (127)' = 577 + 127 = (1, 2, 3, 5) + (1, 2, 1, 6) = (2, 4, 4, 0).$$

Page 24.

Example. $N_1 = 46$, $N_2 = -81$.

$$N_1' = (1, 2, 3, 5) - (1, 1, 4, 2) = (2, 3, 0, 7),$$
$$N_2' = (1, 2, 3, 5) - (0, 1, 4, 4) = (1, 1, 6, 1),$$
$$(N_1 + N_2)' = (2, 3, 0, 7) - (1, 1, 6, 1) - (2, 3, 4, 6) = (2, 2, 3, 3).$$

By checking by transition to the decimal system we obtain

$$(46 - 81)' = (-35)' = 577 - 35 = (1, 2, 3, 5) - (2, 0, 0, 2) = (2, 2, 3, 3).$$

Example. $N_1 = -46$, $N_2 = -81$. By transition to the artificial form:

$$N_1' = (1, 2, 3, 5) - (1, 1, 4, 2) = (0, 1, 6, 3),$$
$$N_2' = (1, 2, 3, 5) - (0, 1, 4, 4) = (1, 1, 6, 1),$$
$$(N_1 + N_2)' = (0, 1, 6, 3) + (1, 1, 6, 1) + (2, 3, 4, 6) = (0, 0, 2, 10).$$

We carry out testing in the decimal system

$$(-46 - 81)' = (-127)' =$$
$$= 577 - 127 = (1, 2, 3, 5) - (1, 2, 1, 6) = (0, 0, 2, 10).$$

Let us give the examples, which illustrate method presented above of conducting the subtraction.

Example. $N_1 = 116$, $N_2 = 87$. We convert/transfer to the artificial form

$$N_1' = (1, 2, 3, 5) - (2, 1, 4, 6) = (0, 3, 0, 0),$$
$$N_2' = (1, 2, 3, 5) - (0, 2, 3, 10) = (1, 4, 6, 4).$$

We form the two's complement of the subtrahend N'_2:

$$(-N_2)' = (2, 4, 6, 10) - (1, 4, 6, 4) = (1, 0, 0, 6).$$

We carry out addition according to (1.16)

$$(N_1 - N_2)' = (N_1 + (-N_2))' = N_1' + (-N_2)' + \overline{\frac{\mathscr{P}-1}{2}} =$$
$$= (0, 3, 0, 0) + (1, 0, 0, 6) + (2, 3, 4, 6) = (0, 1, 4, 1).$$

We check by transition to the decimal system, that

$$(116 - 87)' = (29)' = 577 \div 29 = (1, 2, 3, 5) \div (2, 4, 1, 7) = (0, 1, 4, 1).$$

Example. $N_1 = 116$, $N_2 = -87$.

$$N_1' = (1, 2, 3, 5) - (2, 1, 4, 6) = (0, 3, 0, 0),$$
$$N_2' = (1, 2, 3, 5) - (0, 2, 3, 10) = (1, 0, 0, 6).$$

Let us determine the two's complement of the subtrahend

$$(-N_2)' = (2, 4, 6, 10) - (1, 0, 0, 6) = (1, 4, 6, 4)$$

is produced the addition

$$(N_1 - N_2)' = (0, 3, 0, 0) + (1, 4, 6, 4) + (2, 3, 4, 6) = (0, 0, 3, 10).$$

We check in the decimal system, that

$$(116-(-87))' = (203)' = 577 + 203 = (1, 2, 3, 5) + (2, 3, 0, 5) = (0, 0, 3, 10).$$

Page 25.

Example. $N_1 = -116$, $N_2 = 87$.

$$N_1' = (1, 2, 3, 5) - (2, 1, 4, 6) = (2, 1, 6, 10),$$
$$N_2' = (1, 2, 3, 5) + (0, 2, 3, 10) = (1, 4, 6, 4),$$
$$(-N_2)' = (2, 4, 6, 10) - (1, 4, 6, 4) = (1, 0, 0, 6),$$
$$(N_1 - N_2)' = (2, 1, 6, 10) + (1, 0, 0, 6) + (2, 3, 4, 6) = (2, 4, 3, 0).$$

We check in the decimal system, that

$$(-116-87)' = (-203)' = 577 - 203 =$$
$$= (1, 2, 3, 5) - (2, 3, 0, 5) = (2, 4, 3, 0).$$

Example. $N_1 = -116$, $N_2 = -87$. We will use the results of the previous examples

$$(N_1 - N_2)' = (2, 1, 6, 10) + (1, 4, 6, 4) + (2, 3, 4, 6) = (2, 3, 2, 9).$$

Checking

$$(-116-(-87))' = (-29') = 577 - 29 =$$
$$= (1, 2, 3, 5) - (2, 4, 1, 7) = (2, 3, 2, 9).$$

Let us examine the execution of the operation/process of multiplication during the representation of multipliers in the generalized artificial form.

$$N_1' = \frac{\mathscr{P}-1}{2} + N_1 \quad \text{and} \quad N_2' = \frac{\mathscr{P}-1}{2} + N_2.$$

then

$$N_1' N_2' = \frac{\mathscr{P}-1}{2}\left(N_1 + N_2 + \frac{\mathscr{P}-1}{2}\right) + N_1 N_2.$$

After designating

$$\varphi = N_1 + N_2 + \frac{\mathscr{P}-1}{2},$$

we will obtain

$$N_1' N_2' = \frac{\mathscr{P}-1}{2}\varphi + N_1 N_2,$$

whence

$$(N_1 N_2)' = \frac{\mathscr{P}-1}{2} + N_1' N_2' - \frac{\mathscr{P}-1}{2}\varphi. \qquad (1.17)$$

Assuming/setting

$$\varphi = 2\left[\frac{\varphi}{2}\right] + 2\left\{\frac{\varphi}{2}\right\}$$

(by recording in the curly braces is indicated fractional part of the division φ into two), we will obtain

$$(N_1 N_2)' = \frac{\mathscr{P}-1}{2} + N_1' N_2' + \left[\frac{\varphi}{2}\right] - 2\left\{\frac{\varphi}{2}\right\}\frac{\mathscr{P}-1}{2}.$$

Page 26. If φ is even, then $[\varphi/2] = \varphi/2$ and $\{\varphi/2\} = 0$, then

$$(N_1 N_2)' = \frac{\mathscr{P}-1}{2} + N_1' N_2' + \frac{\varphi}{2}. \qquad (1.18)$$

If φ is odd, then $[\varphi/2] = \varphi - 1/2$ and $\{\varphi/2\} = 1/2$, then

$$(N_1 N_2)' = N_1' N_2' + \frac{\varphi-1}{2}. \qquad (1.19)$$

Let us introduce value t, determined as follows:

$$t = \begin{cases} \dfrac{\varphi}{2}, & \text{(1)} \quad \text{если} \quad \varphi \quad \text{четное,} \\ \dfrac{\varphi - \mathscr{P}}{2}, & \text{(2)} \quad \text{если} \quad \varphi \quad \text{нечетное.} \end{cases}$$

Key: (1). if φ even. (2). if φ odd.

Then expressions (1.18) and (1.19) are transformed into the following:

$$(N_1 N_2)' = \frac{\mathscr{P} - 1}{2} + N_1' N_2' + t. \qquad (1.20)$$

Value φ it is expedient to select expressed through the artificial forms of cofactors, i.e.,

$$\varphi = N_1' + N_2' + \overline{\frac{\mathscr{P} - 1}{2}}. \qquad (1.21)$$

Let us examine some examples, which illustrate the execution of the operation/process of the multiplication when numbers are represented in the artificial form.

Example. $N_1 = 23$, $N_2 = 19$. We convert/transfer to the artificial forms of the cofactors

$$N_1' = (1, 2, 3, 5) + (2, 3, 2, 1) = (0, 0, 5, 6),$$
$$N_2' = (1, 2, 3, 5) + (1, 4, 5, 8) = (2, 1, 1, 2).$$

Let us compute value f according to (1.21):

$$\varphi = (0, 0, 5, 6) + (2, 1, 1, 2) + (2, 3, 4, 6) = (1, 4, 3, 3),$$
$$t = \frac{\varphi}{2} = (2, 2, 5, 7),$$
$$(N_1 N_2)' = (1, 2, 3, 5) + (0, 0, 5, 6) \cdot (2, 1, 1, 2) + (2, 2, 5, 7) =$$
$$= (1, 2, 3, 5) + (0, 0, 5, 1) + (2, 2, 5, 7) = (0, 4, 6, 2).$$

We carry out testing in the decimal system

$$(23 \cdot 19)' = (437)' = 577 + 437 = (1, 2, 3, 5) + (2, 2, 3, 8) = (0, 4, 6, 2)$$

Page 27.

Example. $N_1 = 23$, $N_2 = -19$. Let us compute the artificial forms of the cofactors

$$N_1' = (1, 2, 3, 5) + (2, 3, 2, 1) = (0, 0, 5, 6),$$
$$N_2' = (1, 2, 3, 5) - (1, 4, 5, 8) = (0, 3, 5, 8);$$

let us determine φ:

$$\varphi = (0, 0, 5, 6) + (0, 3, 5, 8) + (2, 3, 4, 6) = (2, 1, 0, 9),$$

hence

$$t = \frac{\varphi}{2} = (1, 3, 0, 10).$$

We compute product on (1.20)

$$(N_1 N_2)' = (1, 2, 3, 5) + (0, 0, 5, 6) \cdot (0, 3, 5, 8) + (1, 3, 0, 10) = (2, 0, 0, 8).$$

We check by transition to the decimal system, that

$$(23 \cdot (-19))' = (-437)' = 577 - 437 =$$
$$= (1, 2, 3, 5) - (2, 2, 3, 8) = (2, 0, 0, 8).$$

Example. $N_1 = -22$, $N_2 = 19$. We convert/transfer to the artificial forms of the cofactors

$$N'_1 = (1, 2, 3, 5) - (1, 2, 1, 0) = (0, 0, 2, 5),$$
$$N'_2 = (1, 2, 3, 5) + (1, 4, 5, 8) = (2, 1, 1, 2).$$

We compute φ:

$$\varphi = (0, 0, 2, 5) + (2, 1, 1, 2) + (2, 3, 4, 6) = (1, 4, 0, 2),$$

hence

$$t = \frac{\varphi}{2} = (2, 2, 0, 1).$$

We compute product in accordance with (1.20)

$$(N_1 N_2)' = (1, 2, 3, 5) + (0, 0, 2, 5) \cdot (2, 1, 1, 2) + (2, 2, 0, 1) = (0, 4, 5, 5).$$

We carry out testing in the decimal system

$$((-22) \cdot 19)' = (-418)' = 577 - 418 =$$
$$= (1, 2, 3, 5) - (1, 3, 5, 0) = (0, 4, 5, 5).$$

Example. $N_1 = -22$, $N_2 = -19$. We compute φ, utilizing the artificial forms of cofactors, determined in the previous examples:

$$\varphi = (0, 0, 2, 5) + (0, 3, 5, 8) + (2, 3, 4, 6) = (2, 1, 4, 8),$$

hence

$$t = \frac{\varphi}{2} = (1, 3, 2, 4).$$

Let us compute the product

$$(N_1 N_2)' = (1, 2, 3, 5) + (0, 0, 2, 5) \cdot (0, 3, 5, 8) + (1, 3, 2, 4) = (2, 0, 1, 5).$$

We check by transition to the decimal system, that

$$((-22)(-19))' = (418)' = 577 + 418 =$$
$$= (1, 2, 3, 5) + (1, 3, 5, 0) = (2, 0, 1, 5).$$

Page 28.

§ 1.5. Multi-stage system of residual classes.

One of the essential advantages of the system of residual classes is the possibility of the parallel processing of the digits, which are remainders/residues along the adopted system of bases/bases $p_1, p_2, \ldots, p_n$. Since in this case the range of the representation of numbers $\mathscr{P}$ is defined as the product of the bases/bases

$$\mathscr{P} = p_1 p_2 \ldots p_n,$$

then it is logical that the range of the representation of numbers increases considerably more rapid than the word format, necessary for the representation of a number, characterized by the sum of the digits, necessary for the representation of remainders/residues according to the selected bases/bases.

The requirement of mutual simplicity of bases/bases does not make it possible to select them clustered in the small section of the series/row of natural numbers. Thus, for instance, one of the possible systems of bases/bases, which realizes the numerical range of order $\mathscr{P} \approx 10^{17}$, will be such 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

It is easy to see that for storing the remainders/residues on

these bases/bases will be required the binary registers with the discharge/digital configuration with respect 2, 3, 3, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6.

On the six-bit registers can be stored the remainders/residues on three more bases/bases of the same series/row, namely on bases/bases 53, 59, 61 which will increase range to the values of order 10^{22}. For further increase of range will be required the transition to the seven-digit registers.

Possibly, the system of bases/bases indicated is not optimum, but it, just as any other, it is reflected/represented natural tendency toward an increase in the discharge/digital configuration of registers with an increase in the numerical range. An increase in the discharge/digital configuration of the registers, which store the remainders/residues of numbers of the examined range, respectively leads to the complication of the equipment for arithmetic unit and an increase in the operation time.

Tendency as far as possible to decrease the value of bases/bases led to the thought to construct the system of residual classes into several steps/stages.

The principal system of the foundations for eating $p_1, p_2, \ldots, p_n$,

and this system of bases/bases provides the possibility of the
execution of operations/processes in preset range $[0, \mathcal{I})$.

Page 24.

The maximum number, which can be obtained in this system with the
multiplication of single digits, exists $(p_n - 1)^2$

We will now represent all digits of principal system in the new
system with bases/bases $\pi_1, \pi_2, \ldots, \pi_r$ by such, that

$$\pi = \pi_1 \pi_2 \ldots \pi_r = (p_n - 1)^2.$$

In this system the maximum number which can be obtained with the
multiplication of its digits, will be number $(\pi_r - 1)^2$ It is possible,
in turn, these last figures (in system $\pi_1, \ldots, \pi_r$) to write record in
the system with bases/bases $\rho_1, \rho_2, \ldots, \rho_s$ under condition
$\rho = \rho_1 \rho_2 \ldots \rho_s = (\pi_r - 1)^2$ and so forth.

This process of transition to the smaller bases/bases noticeably
simplifies the realization of elementary arithmetic unit and is
shortened the time of the execution of arithmetic operation.

Actually/really, for the system with range $\mathcal{I} \leqslant 10^{12}$ the greatest
basis/base is $p_n = 47$.

with the multiplication the greatest number whose
remainder/residue is intended to determine, it can be $46^2=2116$. This,
the second step/stage of the system of residual classes must be such
that its range $\pi = \pi_1\pi_2\ldots\pi_n$ would satisfy for the senior basis/base
condition $\pi>2116$.

Using system proposed above of bases/bases, it is possible
values π_i to select by the following: 3, 5, 11, 13.

The range of the second step/stage for the greatest basis/base
is limited to greatest basis/base $\pi_{max} = 13$

It is possible to examine third step/stage, into which the great
obtained number will be $12^2=144$. It is logical that for the
realization of the third step/stage will be required the bases/bases
of smaller discharge/digital configuration. In particular, from the
same series/row can be selected the system of bases/bases 3, 5, 11.

Here the greatest result of operation will be defined as
$10^2=100$, i.e., for the realization of possible operations/processes
in the fourth step/stage will be required bases/bases 3, 5, 7.

It is obvious that further decrease of the value of the greatest
basis/base is limited, since, even if is removed from the selected

number of mutually simple reasons, will seem that the maximum number,
capable of arising in the process of executing the operation/process,
is equal (to 7-1)^2=36, and the new system of mutually simple
bases/bases it can be selected only from series/row 2, 3, 4, 5, 6,
which is impossible.

Page 30.

Thus, from the initial system of bases/bases with greatest basis/base
p_n=47 it is possible to cross three steps/stages to the system of
bases/bases with the greatest basis/base, equal to 7, thanks to which
is provided a decrease of redundancy in the tables of arithmetic
operations and an increase of the high speed of the latter.
Arithmetic unit in this case in will work only in the highest
step/stage and only in the stages of deduction of result the obtained
numbers must be converted into the form, most preferable for the
output/yield.

Should be focused attention on the circumstance that in general
we win in the redundancy one elementary arithmetic unit; however,
with each increase in the step/stage of bases/bases we lose in the
redundancy of entire arithmetic unit due to an increase in the
discharge/digital configuration of entire number and due to an
increase in the redundancy upon transfer to the new step/stage.

Let us examine some examples, which illustrate multilevel systems.

For the operation with numbers from 1 to 10^3 should be selected the system of bases/bases, in which would be represented numbers from 1 to 10^6. It is possible to accept the system of the bases/bases:

$$p_1 = 11, \quad p_2 = 13, \quad p_3 = 17, \quad p_4 = 20, \quad p_5 = 21.$$

Here $\mathscr{P} = p_1 p_2 p_3 p_4 p_5 = 1011020 > 10^6.$.

With the operations/processes with the digits in this system a maximally possible result $20 \cdot 20 = 400$.

We will each of the digits represent in the system with the bases/bases:

$$\pi_1 = 3, \quad \pi_2 = 4, \quad \pi_3 = 5, \quad \pi_4 = 7.$$

Range of this system

$$\pi = \pi_1 \pi_2 \pi_3 \pi_4 = 3 \cdot 4 \cdot 5 \cdot 7 = 420.$$

The greatest possible result in this system will be defined as $(7-1)^2 = 36$, while in the first system of bases/bases the greatest possible result was equal to 400, i.e., here elementary arithmetic unit operates with numbers, 10 times less in the value.

Example. Assume we should conduct multiplication 115·541. Let us write cofactors in the principal system of bases/bases (first stage)

$$115 = (5, 11, 13, 15, 10); \quad 541 = (2, 8, 14, 1, 16).$$

Let us write now these numbers in the system of the bases/bases of the following (second) step/stage:

$$115 = [(2, 1, 0, 5); (2, 3, 1, 4); (1, 1, 3, 6); (0, 3, 0, 1); (1, 2, 0, 3)],$$
$$541 = [(2, 2, 2, 2); (2, 0, 3, 1); (2, 2, 4, 0); (1, 1, 1, 1); (1, 0, 1, 2)].$$

Let us produce multiplication in the second step/stage

$$115 \cdot 541 = [(1, 2, 0, 3); (1, 0, 3, 4); (2, 2, 2, 0); (0, 3, 0, 1); (1, 0, 0, 6)].$$

Page 31.

Let us examine how appears the obtained result in first stage:

$$115 \cdot 541 = (10, 88, 182, 15, 160).$$

Operations/processes in the lowest system will always be correct, if true result does not leave the range of the representation of numbers of senior step/stage. In this case also must not have point of emergence from the range of the representation of numbers and in the lowest step/stage.

Returning to the result of the multiplication conducted, let us lead it to the smallest positive remainders/residues along the selected system of the bases/bases

$$115 \cdot 541 = (10, 10, 12, 15, 13) = 62215.$$

Example. Compute 41^2.   Let us write number 41 in the first

system cf the bases/bases

$$41 = (8, 2, 7, 1, 20).$$

Let us pass to the second step/stage

$$41 = [(2, 0, 3, 1); (2, 2, 2, 2); (1, 3, 2, 0); (1, 1, 1, 1); (2, 0, 0, 6)].$$

Let us elevate 41 into the square in the second step/stage

$$41^2 = [(1, 0, 4, 1); (1, 4, 4, 4); (1, 1, 4, 0); (1, 1, 1, 1); (1, 0, 0, 1)].$$

Let us restore/reduce result in first stage

$$41^2 = (64, 4, 49, 1, 400)$$

and let us lead it to the smallest positive remainders/residues in first stage

$$41^2 = (9, 4, 15, 1, 1,) = 1681.$$

§ 1.6. Rational operations/processes in the system of residual classes.

Above it was established/installed, that the operations/processes of addition and multiplication on the numbers, represented in the system of residual classes, are reduced to the appropriate operations/processes above the digits of this representation. This proves to be valid also for any complex operations/processes, comprised cf the operations/processes of addition and multiplication. Sole limitation in the fulfillment of this type of complicated operations/processes is the requirement of nonappearance beyond the limits cf range, determined by the basis of

system accepted both final, and intermediate results. With some refined rules of the fulfillment of complicated operations/processes it proves to be possible to be limited by the requirement of nonappearance from the range only of final result, leaving after the intermediate results the possibility to exceed the limits of range.

Page 32.

It is obvious that the aforesaid relates also to the calculation of the values of polynomial.

Let be given polynomial $Q(x)$:

$$Q(x) = \sum_{i=0}^{r} a_i x^i,$$

where

$$a_i = (\alpha_1^{(i)}, \alpha_2^{(i)}, \ldots, \alpha_n^{(i)});$$
$$x^i = (x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)});$$

coefficients and the degree of basing of polynomial, presented in the system of residual classes on bases/bases p_1, p_2, ..., p_n. Let us designate through $Q_j(x_j)$ the expression

$$Q_j(x_j) = \sum_{i=0}^{r} \alpha_j^{(i)} x_j^{(i)}.$$

Then in accordance with the rules of addition and multiplication in the system of the residual classes

$$Q(x) = \left(\sum_{i=0}^{r} \alpha_1^{(i)} x_1^{(i)}; \quad \sum_{i=0}^{r} \alpha_2^{(i)} x_2^{(i)}; \quad \ldots; \quad \sum_{i=0}^{r} \alpha_n^{(i)} x_n^{(i)} \right) =$$
$$= (Q_1(x_1), \ Q_2(x_2), \ \ldots, \ Q_n(x_n)). \qquad (1.22)$$

The components of polynomials are written/recorded taking into account signs in the artificial form.

For the illustration let us examine some examples. In these examples is accepted the system of the bases/bases: $p_1=2$, $p_2=3$, $p_3=5$, $p_4=7$.

Example. Compute expression AB+C with A=4, B=5, C=-3.

Let us write the preset numbers in the artificial form:

$$A' = (1, 0, 0, 0) + (0, 1, 4, 4) = (1, 1, 4, 4)$$
$$B' = (1, 0, 0, 0) + (1, 2, 0, 5) = (0, 2, 0, 5),$$
$$C' = (1, 0, 0, 0) - (1, 0, 3, 3) = (0, 0, 2, 4).$$

We compute expression A'•B'+C':

$$A' \cdot B' + C' = (1, 1, 4, 4) \cdot (0, 2, 0, 5) + (0, 0, 2, 4) = (0, 2, 2, 3).$$

Let us perform testing in the decimal system

$$(4 \cdot 5 - 3)' = (17)' = 105 + 17 = (1, 0, 0, 0) - (1, 2, 2, 3) = (0, 2, 2, 3).$$

Example. Compute expression AB+C with A=5, B=-3, C=4.

Let us lead the preset numbers to the artificial form:

$$A' = (1, 0, 0, 0) + (1, 2, 0, 5) = (0, 2, 0, 5),$$
$$B' = (1, 0, 0, 0) - (1, 0, 3, 3) = (0, 0, 2, 4),$$
$$C' = (1, 0, 0, 0) + (0, 1, 4, 4) = (1, 1, 4, 4).$$

Page 33.

We compute expression A'•B'+C':

$$A' \cdot B' + C' = (0, 2, 0, 5)(0, 0, 2, 4) + (1, 1, 4, 4) + (1, 0, 0, 0) =$$
$$= (1, 1, 4, 3) + (1, 0, 0, 0) = (0, 1, 4, 3).$$

We check in the decimal system, that

$$(5 \cdot (-3) + 4)' = (-11)' = 105 - 11 =$$
$$= (1, 0, 0, 0) - (1, 2, 1, 4) = (0, 1, 4, 3).$$

Example. Compute expression (A-B)C with A=17, B=7, C=5.

Let us write the preset numbers in the artificial form:

$$A' = (1, 0, 0, 0) - (1, 2, 2, 3) = (0, 2, 2, 3),$$
$$B' = (1, 0, 0, 0) + (1, 1, 2, 0) = (0, 1, 2, 0) - B' =$$
$$= (2, 3, 5, 7) - (0, 1, 2, 0) = (0, 2, 3, 0).$$
$$C' = (1, 0, 0, 0) + (1, 2, 0, 5) = (0, 2, 0, 5).$$

We compute expression (A'-B')C':

$$(A' - B') C' = ((0, 2, 2, 3) + (0, 2, 3, 0) + (1, 0, 0, 0)) \cdot (0, 2, 0, 5) -$$
$$+ (1, 0, 0, 0) = (1, 1, 0, 3)(0, 2, 0, 5) - (1, 0, 0, 0) = (1, 2, 0, 1).$$

We carry out testing in the decimal system

$$((17 - 7) \cdot 5)' = (50)' = 105 + 50 = (1, 0, 0, 0) - (0, 2, 0, 1) = (1, 2, 0, 1).$$

Example. Compute the value of polynomial $Q(x) = 11x^2 - 7x + 3$ with

x=3.

Let us write $Q(x)$ with the coefficients represented in the artificial form:

$$Q'(x) = (0, 2, 1, 4) x^2 - (0, 2, 3, 0) x - (1, 2, 3, 1),$$
$$x' = (1, 0, 0, 0) + (1, 0, 3, 3) = (0, 0, 3, 3).$$

We compute values $Q_j(x_j)$, where x_j - remainder/residue on basis/base p_j:

$$Q_1(x_1) = 0 \cdot 0^2 + 0 \cdot 0 + 1 = 1,$$
$$Q_2(x_2) = 2 \cdot 0^2 + 2 \cdot 0 + 2 = 2,$$
$$Q_3(x_3) = 1 \cdot 3^2 + 3 \cdot 3 + 3 = 1,$$
$$Q_4(x_4) = 4 \cdot 3^2 + 0 \cdot 3 + 1 = 2.$$

Hence

$$Q'(x') = (1, 2, 1, 2).$$

We check in the decimal system

$$(Q(3))' = 105 + Q(3) = 105 + 86 = (1, 0, 0, 0) + (0, 2, 1, 2) = (1, 2, 1, 2)$$

§ 1.7. Translation of numbers of the positional system into the system of residual classes and vice versa.

The translation/conversion of number N from the positional system into the system of residual classes can be realized with the aid of the set of the constants, which are the equivalents of degrees p (basis of positional system) in the system of residual classes.

Let number N be preset in the positional numeration system with basis/base p

$$N = a_r p^r + a_{r-1} p^{r-1} + \ldots + a_1 p + a_0$$

or

$$N = \sum_{i=0}^{r} a_i p^i. \qquad (1.23)$$

Here a_i - one of the numbers $0, 1, 2, \ldots, p-1$ and let

$$p^i = (\beta_1^{(i)}, \beta_2^{(i)}, \ldots, \beta_n^{(i)}) \quad \text{for} \quad i = 1, 2, \ldots, r$$

- be the representations of degrees of p in the system of residual classes with bases/bases $p_1, p_2, \ldots, p_n$, and value

$$a_i = (\alpha_1^{(i)}, \alpha_2^{(i)}, \ldots, \alpha_n^{(i)}) \quad \text{for} \quad i = 1, 2, \ldots, r$$

- representation of the coefficients of polynomial (1.23) in the system of residual classes. Then in accordance with (1.22) it is possible to easily form number N in the system of residual classes. After designating

$$Q_j = \sum_{i=0}^{r} \alpha_j^{(i)} \beta_j^{(i)},$$

we will obtain

$$N = (Q_1, Q_2, \ldots, Q_n). \qquad (1.24)$$

i.e. for forming the number N in the system of residual classes it is required knowledge r of the constants, which are degrees of p and p-1

constants of appropriate for possible values a_i i.e. in all $r+p$
constants. This path is simpler than direct indexing N into each
basis/base and formation/education of remainder/residue, as this
escape/ensues from the determination of system. It can be realized in
the presence of the arithmetic unit, which works in the system of
residual classes.

Example. To translate number 102 of the decimal system into the
system of residual classes with the bases/bases: $p_1=3$, $p_2=5$, $p_3=7$.

Let us extract constants:

$$p^0 = 1 = (1, 1, 1), \quad p^1 = 10 = (1, 0, 3), \quad p^2 = 100 = (1, 0, 2);$$
$$a_0 = 2 = (2, 2, 2), \quad a_1 = 0 = (0, 0, 0), \quad a_2 = (1, 1, 1).$$

then in accordance with (1.24)

$$102 = (2 \cdot 1 - 0 \cdot 1 - 1 \cdot 1, 2 \cdot 1 - 0 \cdot 0 - 1 \cdot 0, 2 \cdot 1 + 0 \cdot 3 + 1 \cdot 2) = (0, 2, 4).$$

Page 35.

Possible if does not limit storage, to have a set of constants
of the values of products $a_j p^j$ (j=0, 1, ..., p-1) in the system of
residual classes.

tb then number N is formed simply by the additions of the
corresponding constants.

Calculation N can also be conducted according to the diagram of Horner for the polynomial.

Let us examine now translation algorithm from the system of residual classes into the positional system.

Let the basis of the system of residual classes be p_1, $p_2, \ldots, p_n$. Let us assign n of numbers $B_1, B_2, \ldots, B_n$ in the system of the residual classes

$$B_j = (\beta_1^{(j)}, \beta_2^{(j)}, \ldots, \beta_n^{(j)}).$$
$$j = 1, 2, \ldots, n,$$

which subsequently we will call the basis of system. As it will be evidently further, the bases of system are its basic constants. Their values are defined simultaneously with the selection of system and are known to us both in the system of residual classes and in the positional numeration system.

Let for the translation/conversion into the positional system be is preset number A in the form

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n).$$

The goal of translation/conversion consists in determining of numbers $\mu_1, \mu_2, \ldots, \mu_n$ such, that

$$\mu_1 B_1 + \mu_2 B_2 + \ldots + \mu_n B_n = A. \qquad (1.25)$$

Let us rewrite (1.25) in the system of the residual classes

$$\mu_1 (\beta_1^{(1)}, \beta_2^{(1)}, \ldots, \beta_n^{(1)}) + \mu_2 (\beta_1^{(2)}, \beta_2^{(2)}, \ldots, \beta_n^{(2)}) + \ldots$$
$$\ldots + \mu_n (\beta_1^{(n)}, \beta_2^{(n)}, \ldots, \beta_n^{(n)}) = (\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Equalizing corresponding remainders/residues, we obtain the system of linear algebraic equations for determining the values $\mu_1, \mu_2, \ldots, \mu_n$:

$$\left.\begin{array}{l} \mu_1 \beta_1^{(1)} + \mu_2 \beta_1^{(2)} + \ldots + \mu_n \beta_1^{(n)} = \alpha_1, \\ \mu_1 \beta_2^{(1)} + \mu_2 \beta_2^{(2)} + \ldots + \mu_n \beta_2^{(n)} = \alpha_2, \\ \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \\ \mu_1 \beta_n^{(1)} + \mu_2 \beta_n^{(2)} + \ldots + \mu_n \beta_n^{(n)} = \alpha_n. \end{array}\right\} \qquad (1.26)$$

Page 36.

System (1.26) will have the whole solutions, if the determinant of system is equal to $+-1$, i.e.,

$$\begin{vmatrix} \beta_1^{(1)}, \beta_1^{(2)}, \ldots, \beta_1^{(n)} \\ \beta_2^{(1)}, \beta_2^{(2)}, \ldots, \beta_2^{(n)} \\ \cdots \cdots \cdots \cdots \\ \beta_n^{(1)}, \beta_n^{(2)}, \ldots, \beta_n^{(n)} \end{vmatrix} = \pm 1. \qquad (1.27)$$

There is a large selection of values $\beta_1, \beta_2, \ldots, \beta_n$, since any system of values $\beta_j^{(i)}$ is acceptable as the remainders/residues of bases, if it satisfies condition (1.27).

In the particular case as the bases of system can be selected the following values

$$B_1 = (1, 0, 0, \ldots, 0), \quad B_2 = (0, 1, 0, \ldots, 0), \ldots$$
$$\ldots, B_n = (0, 0, \ldots, 1), \qquad (1.28)$$

which it is logical to call the orthogonal bases of system. In accordance with (1.26) for the orthogonal bases we obtain

$$\mu_i = \alpha_i \quad \text{for} \quad i = 1, 2, \ldots, n, \qquad (1.29)$$

whence

$$A = \alpha_1 B_1 + \alpha_2 B_2 + \ldots + \alpha_n B_n \quad (\text{mod } \mathscr{P}). \qquad (1.30)$$

For these bases the determinant of left side takes the form

$$\begin{vmatrix} 100 \ldots 0 \\ 010 \ldots 0 \\ \cdot \cdot \cdot \cdot \cdot \\ 000 \ldots 1 \end{vmatrix} = 1.$$

Let us examine an example of the use/application of orthogonal bases for the translation/conversion from the system of residual classes with bases/bases $p_1 = 3$, $p_2 = 5$, $p_3 = 7$ into the decimal system.

Example. To translate number $A = (2, 3, 5)$ into the decimal system.

Let us extract the orthogonal bases:

$$B_1 = (1, 0, 0) = 70, \quad B_2 = (0, 1, 0) = 21, \quad B_3 = (0, 0, 1) = 15.$$

On the basis (1.30) it is possible to write

$$A = (2, 3, 5) = 2B_1 - 3B_2 + 5B_3 = 2 \cdot 70 - 3 \cdot 21 + 5 \cdot 15 = 278.$$

The obtained result is introduced into the range by the subtraction of value, multiple $*$ 105 and finally we obtain

$$A \quad (2, 3, 5) \quad 278 - 2 \cdot 105 = 68.$$

Page 37.

Regarding orthogonal bases (1.28) they can be represented in the form

.

$$B_i = \frac{m_i \mathscr{P}}{p_i} \text{ for } i = 1, 2, \ldots, n,$$

where m_i - whole positive number which let us name/call the weight of orthogonal basis.

Moreover m_i must be selected in such a way that would occur the following comparison

$$\frac{m_i \mathscr{P}}{p_i} \equiv 1 \,(\text{mod } p_i \qquad\qquad (1 \; 31)$$

or

$$\frac{m_i \mathscr{P}}{p_i} = l_i p_i + 1,$$

where l_i - positive integer number.

Let us point out, how it is expedient to compute value m_i. Let us introduce designation $\mathscr{P}_i = \frac{\mathscr{P}}{p_i}$. Let us compute $\mathscr{P}_i = \frac{\mathscr{P}}{p_i}$. We divide $\mathscr{P}_i$ into

p_i. Since $\mathcal{P}_i$ of the multipliers of mutually simple ones with p_i, that $\mathcal{P}_i$, it will not be comprised completely divided into p_i, as a result of division we will obtain certain remainder/residue which let us designate through δ_i. Then in accordance with (1.31) m_i is defined as the solution of the comparison

$$m_i \delta_i \equiv 1 \;(\bmod\; p_i). \qquad (1.32)$$

In view of a comparative smallness of values of bases/bases for set p_i it is possible to make table of the solutions of comparisons (1.32), in which through value δ_i is located appropriate m_i. Assuming that the basis of system are taken by simple ones, let us give the tables of the solutions of comparison (1.32) for the prime numbers in the range 2^6.

In this table for each prime number in the range $1-2^6$ are given m_i, those corresponding to all possible ones δ.

For the check of the calculation of orthogonal bases it is possible to use the relationship/ratio, obtained from (1.28):

$$B_1 + B_2 + \ldots + B_n \approx (1,\, 0,\, \ldots,\, 0) + (0,\, 1,\, \ldots,\, 0) + \ldots +$$
$$+ (0,\, 0,\, \ldots,\, 1) = (1,\, 1,\, \ldots,\, 1) = 1.$$

Since the operation is carried out in the system with range $[0, \mathcal{P})$, the control relationship/ratio can be written as

$$\sum_{i=1}^{n} B_i \equiv 1 \;(\bmod\; \mathcal{P}). \qquad (1.33)$$

Page 38.

Table of the solutions of comparison (1.32).

δ \ p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2		2	3	4	6	7	9	10	12	15	16	19	21	22	24	27	30	31
3			2	5	4	9	6	13	8	10	21	25	14	29	16	18	20	41
4			4	2	3	10	13	5	6	22	8	28	31	11	12	40	15	46
5				3	9	8	7	4	14	6	25	15	33	26	19	32	12	49
6				6	2	11	3	16	4	5	26	31	7	36	8	9	10	51
7					8	2	5	11	10	25	9	16	6	37	27	38	17	35
8					7	5	15	12	3	11	4	14	36	27	6	20	37	23
9					5	3	2	17	18	13	7	33	32	24	21	6	46	34
10					10	4	12	2	7	3	28	26	37	13	33	16	6	55
11						6	14	7	21	8	17	27	15	4	30	29	43	50
12						12	10	8	2	17	13	24	24	18	4	31	5	56
13							4	3	16	9	12	20	19	10	29	49	50	47
14							11	15	5	27	20	8	3	40	37	19	38	48
15							8	14	20	2	29	5	11	23	22	46	4	57
16							16	6	13	20	2	7	18	35	3	10	48	42
17								9	19	12	11	24	29	38	36	25	7	18
18								18	9	21	19	35	16	12	34	3	23	17
19									17	26	18	2	13	34	5	14	28	45
20									15	16	14	13	39	28	40	8	3	58
21									11	18	3	30	2	41	9	48	45	32
22									22	4	24	32	28	2	15	41	51	25
23										24	27	29	25	15	45	30	18	8
24										23	22	17	12	9	2	42	32	28
25										7	5	3	23	31	32	17	26	22
26										19	6	10	30	5	38	51	25	54
27										14	23	11	38	8	7	2	35	52
28										28	10	4	22	20	42	36	19	24
29											15	23	17	3	13	11	57	40
30											30	21	26	33	11	23	2	59
31												6	4	25	44	12	40	2
32												22	9	39	25	5	24	21
33												9	5	30	10	45	34	37
34												12	35	19	18	39	33	9
35												18	34	16	43	50	27	7
36												36	8	6	17	28	41	39
37													10	7	14	43	8	33
38													27	17	26	7	14	53
39													20	32	41	34	56	36
40													40	40	20	4	31	29
41														21	39	22	36	3
42														42	28	24	52	16
43															35	37	11	44
44															31	47	55	43
45															23	33	21	19
46															46	15	9	4
47																14	54	13

δ \ p	53	59	61
48	21	16	14
49	13	53	5
50	35	13	11
51	26	22	6
52	52	42	27
53		49	38
54		47	26
55		44	10
56		56	12
57		29	15
58		58	20
59			30
60			60

Page 39.

Let us examine examples of the calculation of orthogonal bases, utilizing data from the table.

Example. Let be given the system of the bases/bases:

$$p_1 = 3, \quad p_2 = 5, \quad p_3 = 7, \quad p_4 = 17. \quad \mathscr{P} = p_1 p_2 p_3 p_4 = 1785.$$

We compute:

$$\frac{\mathscr{P}}{p_1} = 5 \cdot 7 \cdot 17 = 595, \qquad \frac{\mathscr{P}}{p_2} = 3 \cdot 7 \cdot 17 = 357,$$

$$\frac{\mathscr{P}}{p_3} = 3 \cdot 5 \cdot 17 = 255, \qquad \frac{\mathscr{P}}{p_4} = 3 \cdot 5 \cdot 7 = 105.$$

We compute now:

$$\delta_1 = \frac{595}{3} \pmod 3 = 1, \qquad \delta_2 = \frac{357}{5} \pmod 5 = 2,$$

$$\delta_3 = \frac{255}{7} \pmod 7 = 3, \qquad \delta_4 = \frac{105}{17} \pmod{17} = 3.$$

Through the table we find: $m_1 = 1$, $m_2 = 3$, $m_3 = 5$, $m_4 = 6$. Thus,

$$B_1 = 1 \cdot 595 = 595, \qquad B_2 = 357 \cdot 3 = 1071,$$

$$B_3 = 5 \cdot 255 = 1275, \qquad B_4 = 6 \cdot 105 = 630.$$

We check against the control relationship/ratio

$$B_1 + B_2 + B_3 + B_4 = 595 + 1071 + 1275 + 630 = 3571;$$
$$3571 - 2 \cdot 1785 = 1.$$

Page 40.

Chapter 2.

Theoretical-numerical bases of the system of residual classes.

§2.1. Elements/cells of the theory of comparisons.

The basic theoretical-numerical basis of the system of residual classes is the theory of comparisons. Questions of the theory of comparisons were worked out by outstanding Russian Scientific P. L. Chebyshev and presented in his classical work "Theory of comparisons". Following in essence P. L. Chebyshev's presentation, will be examined below some questions of the theory of comparisons, necessary for the development of the system of residual classes, and also some methods of executing the arithmetic operations, which are based on the use/application of theory of primitive roots and indices.

Determination. For integers a and b are congruent between

themselves in modulus/module p, if their difference a-b is multiple p

(it is divided completely into p), i.e., a-b=lp, where l - integer.

For the comparison is accepted the designation

$$a \equiv b \pmod{p}. \qquad (2.1)$$

Comparison can be treated as equality on the modulus/module. This

makes sense, since the comparisons possess many properties, inherent

in equalities. Let us enumerate these properties.

Page 41.

Property 1. If a, b, c and p - integers, then from the

comparisons

$$a \equiv c \pmod{p} \text{ and } b \equiv c \pmod{p}$$

it follows that also

$$a \equiv b \pmod{p}, \qquad (2.2)$$

i.e. two numbers, congruent with the third in certain modulus/module,

are congruent between themselves in the same modulus/module.

Actually/really, regarding the comparison

$$a = l_1 p + c \quad \text{и} \quad b = l_2 p - c,$$

where l_1 and l_2 - integers.

After excluding c of both equalities, we will obtain

$$a = (l_1 - l_2) p + b,$$

whence it ensues/escapes/flows out (2.2).

Property 2. In the comparisons, just as in the equalities, it is possible to transfer terms of one part into another without the disturbance/breakdown of comparison.

Let occur the comparison

$$a_1 + a_2 + \ldots + a_m \equiv b_1 + b_2 + \ldots + b_n \,(\text{mod } p).$$

Regarding this indicates the presence of the equality

$$a_1 + a_2 + \ldots + a_m = kp + b_1 + b_2 + \ldots + b_n.$$

Equality will not be broken, if we transfer of one part of it into another, taking into account signs, any quantity of terms. Let we transfer from the left side of the equality members $a_1, a_2, \ldots, a_s$ into the right, and from the right $b_1, b_2, \ldots, b_t$ into the left. Then it is possible to rewrite equality in the form

$$a_{s+1} + \ldots + a_m - b_1 - b_2 - \ldots - b_t$$
$$= kp + b_{t+1} + \ldots + b_n - a_1 - \ldots - a_s.$$

Passing from the equality to the comparison, let us write

$$a_{s+1} + \ldots + a_m - b_1 - \ldots - b_t \equiv$$
$$b_{t+1} + \ldots + b_n - a_1 - \ldots - a_s \,(\text{mod } p).$$

that also shows the validity of the formulated property. In particular, if

$$a \equiv b \,(\text{mod } p), \quad \text{то и} \quad b \equiv a \,(\text{mod } p).$$

Property 3.

$$a_1 \equiv b_1 \,(\text{mod } p) \quad \text{и} \quad a_2 \equiv b_2 \,(\text{mod } p).$$

Page 42.

Then occur and the comparisons

$$a_1 + a_2 \equiv b_1 + b_2 \,(\text{mod } p),$$
$$a_1 - a_2 \equiv b_1 - b_2 \,(\text{mod } p), \qquad (2.3)$$

i.e. comparisons on one and the same modulus/module can be piecemeal stored/added up and subtracted.

The actually/really preset comparisons can be rewritten in the form of the equalities

$$a_1 = k_1 p + b_1 \quad \text{and} \quad a_2 = k_2 p + b_2;$$

by storing/adding up and by subtracting piecemeal these equalities, we will obtain

$$a_1 + a_2 = (k_1 + k_2)\,p + b_1 + b_2,$$
$$a_1 - a_2 = (k_1 - k_2)\,p + b_1 - b_2.$$

After switching over from the equalities to the appropriate comparisons, we will obtain (2.3). This property applies to any quantity of comparisons.

Let us give the illustrating example.

Example. From the comparisons $77 \equiv 5 \,(\text{mod } 8)$, $36 \equiv 4 \,(\text{mod } 8)$ by term-by-term addition - subtraction we obtain the comparisons

$$77 + 36 \equiv 5 + 4 \,(\text{mod } 8), \text{ т. е. } 113 \equiv 9 \,(\text{mod } 8) \quad \text{and}$$
$$77 - 36 \equiv 5 - 4 \,(\text{mod } 8), \text{ т. е. } 41 \equiv 1 \,(\text{mod } 8).$$

validity of which is easily set by testing.

Property 4. If takes the place

$$a \equiv b \,(\mathrm{mod}\,p)$$

and r - integer, then

$$ar \equiv br \,(\mathrm{mod}\,p), \qquad\qquad (2.4)$$

i.e. the members of comparison can be multiplied by one and the same integer.

Actually/really, the first comparison is equivalent to the equality

$$a = kp - b.$$

After multiplying both parts of this equality to r, we will obtain the equality

$$ar = krp + br = Kp + br,$$

where

$$K = kr.$$

which is equivalent (2.4).

Page 43.

Let us illustrate this property by an example.

Example. Occurs comparison $47 \equiv 3 \,(\mathrm{mod}\,11)$. Multiplicand are both

parts of it to 17. We will obtain $799 \equiv 51$ (mod 11). By testing we

establish that $799 - 51 = 748$ is divided by 11.

Property 5.
$$a_1 \equiv b_1 \,(\mathrm{mod}\, p); \ a_2 \equiv b_2 \,(\mathrm{mod}\, p); \ldots; \ a_s \equiv b_s \,(\mathrm{mod}\, p).$$

Then
$$a_1 a_2 \ldots a_s \equiv b_1 b_2 \ldots b_s \,(\mathrm{mod}\, p), \qquad (2.5)$$

i.e. comparisons on one and the same modulus/module can piecemeal be

multiplied to each other.

Actually/really, let us register the comparisons as of s of the

equalities
$$a_1 = k_1 p + b_1; \ a_2 = k_2 p + b_2; \ldots; \ a_s = k_s p + b_s.$$

Multiplying piecemeal these equalities, we will obtain the equality

$$
\begin{aligned}
a_1 a_2 \ldots a_s = k_1 k_2 \ldots k_s p^s &+ (k_1 k_2 \ldots k_{s-1} b_s + \\
+ k_1 k_2 \ldots k_{s-2} k_s b_{s-1} + \ldots &+ k_2 k_3 \ldots k_s b_1) p^{s-1} + \ldots \\
\ldots + (k_1 b_2 b_3 \ldots b_s + k_2 b_1 b_3 \ldots b_s &+ \ldots \\
\ldots + k_s b_1 b_2 \ldots b_{s-1}) p &+ b_1 b_2 \ldots b_s,
\end{aligned}
$$

which is equivalent (2.5).

Property 6. Let be given the polynomial
$$f(x) = g_n x^n + g_{n-1} x^{n-1} + \ldots + g_{n-1} x + g_0$$
with the whole coefficients and let a be is congruent with b in

modulus/module p. Then
$$f(a) \equiv f(b) \,(\mathrm{mod}\, p). \qquad (2.6)$$

i.e. the values of polynomial with the whole coefficients from two arguments, congruent in certain modulus/module, are congruent between themselves in the same modulus/module.

This property is set on the basis of the use of the previous properties of comparisons.

Let us give the illustrating example.

Example. Let be given the polynomial

$$f(x) = 7x^4 - 12x^3 - 23x^2 - 11x - 10$$

and let it be it is given $22 \equiv 7$ (mod 5). Let us find the values of polynomial with $x=2$ and $x=7$

$$f(22) = 1\,788\,952; \quad f(7) = 22\,137.$$

Let us compute the difference

$$f(22) - f(7) = 1\,788\,952 - 22\,137 = 1\,766\,815.$$

It is easy to see that this difference is divided by 5, i.e.

$$f(22) \equiv f(7) \,(\mathrm{mod}\,5).$$

Page 44.

Property 7. Let occur the comparison

$$ac \equiv bc \,(\mathrm{mod}\,p),$$

moreover c is mutually simple with p. Then is performed the comparison
$$\equiv b \,(\mathrm{mod}\,p).$$

i.e. the members of comparison can be abbreviated/reduced to their common factor, if the latter is mutually simple with the modulus/module. Initial comparison is equivalent to the equality

$$ac = kp + bc.$$

Since the left side of the equality is multiple c, then right side also must be multiple c. With p and c mutually simple must be < multiple c i.e.

$$k = lc,$$

then
$$ac = lcp + bc.$$

After shortening both parts of this equality to c, we will obtain

i.e.
$$a = lp + b,$$
$$a \equiv b \pmod{p}.$$

Example. From the comparison $374 \equiv 77$ (mod 9) it follows, after decrease to 11, $34 \equiv 7$ (mod 9), i.e., difference $34-7=27$ is divided by 9.

Property 8. Let occur the comparison

$$ac \equiv bc \pmod{pc}.$$

Then takes the place $a \equiv b \pmod{p}$, .

i.e. the comparison, terms and modulus/module of which have common factor, it can be abbreviated/reduced to this multiplier. Actually/really, after writing the equivalent to initial comparison equality

$$ac = kcp + bc$$

and shortening it on c, we will obtain

$$a \equiv b \, (\text{mod } p).$$

Let us give the illustrating example.

Example. From the comparison $87 \equiv 3 \, (\text{mod } 21)$, by the decrease of its terms and modulus/module to 3, we obtain comparison $29 \equiv 1 \, (\text{mod } 7)$ valid, since $29 - 1 = 28$ it is divided by 7.

Page 45.

§2.2. Solution of the simplest comparisons.

Number x, which satisfies the comparison

$$f(x) \equiv 0 \, (\text{mod } p), \qquad (2.7)$$

let us name the solution of this comparison. From that presented it is clear that if comparison (2.7) has although one solution, then it has countless solution set, congruent with the data by the solution by modulus/module p. Among these solutions t' re is small positive number and a small (in the absolute value) negative number, i.e., the

smallest positive deduction and respectively smallest negative
deduction.

Let us introduce the concept of the independent solutions of
comparison (2.7). Two solutions α and β comparisons we will call the
independent solutions, if they are incomparable between themselves on
modulus/module p. Further, everywhere, speaking about a number of
solutions of comparison (2.7), we will have in mind precisely a
number of independent solutions, since to speak about a number of
dependent solutions does not have a sense - it, as we saw above,
infinitely.

Occurs the following theorem.

Theorem 2.1. The comparison
$$f(x) \equiv 0 \,(\text{mod}\, p)$$
has as many the solutions, as numbers in the series/row
$$0, 1, \ldots, p-1 \qquad (2.8)$$
it they satisfy.

Proof. If we through $\alpha_1, \alpha_2, \ldots, \alpha_n$ designate these numbers,
then a number of solutions will be n and the set of the solutions of
comparison (2.7) can be registered in the form:
$$x \equiv \alpha_1 \,(\text{mod}\, p),$$
$$x \equiv \alpha_2 \,(\text{mod}\, p),$$
$$\cdots \cdots \cdots$$
$$x \equiv \alpha_n \,(\text{mod}\, p).$$

Let us designate through α an arbitrary number of sequence (2.8). Then any number β, which lies out of sequence (2.8), can be registered in the form

$$\beta = kp + \alpha.$$

Let us assume that β is the solution of comparison (2.7), i.e.

$$f(\beta) \equiv 0 \,(\text{mod}\, p).$$

Page 46.

After substituting value β into the right side of the polynomial, we will obtain

$$f(\beta) = Lp + f(\alpha).$$

Whence
$$f(\alpha) \equiv 0 \,(\text{mod}\, p),$$

i.e. α must be the solution of comparison, in other words in one of the numbers α_1, α_2, ..., α_n. But then β as the number, congruent with α, is not the independent solution of comparison (2.7). Thus, the independent, independent solutions there can be not more than p.

Example. Let be given polynomial f(x) of the form

$$f(x) = 3x^3 + 2x^2 + 5x + 2.$$

Substituting in it consecutively/serially for x number 0, 1, 2, 3, ..., 10, we will obtain values of f(x), the respectively equal to 2,

12, 44, 116, 246, 452, 752, 1164, 1706, 2396, 3152, from which are

multiple p=11 only 44, that corresponds to value of x=2.

Thus, the comparison

$$3x^3 + 2x^2 + 5x + 2 \equiv 0 \ (\text{mod } 11)$$

has only one solution of x≡2 (mod 11).

Corollary. Linear congruence

$$ax + b \equiv 0 \ (\text{mod } p) \qquad (2.9)$$

can have only one solution with a≢0 (mod p). Actually/really, all

solutions of this comparison according to the previous theorem must

be located among numbers of sequence (2.8). Let α_1 be such solution.

This means that

$$a\alpha_1 + b = kp. \qquad (2.10)$$

Let there be by α_2 - second solution of this comparison, i.e.

$$a\alpha_2 + b = lp. \qquad (2.11)$$

Subtrahend (2.11) from (2.10). We will obtain

$$a(\alpha_1 - \alpha_2) = (k - l)p. \qquad (2.12)$$

Since the right side of the equality is multiple p, then left side

must be multiple p. But $\alpha_1 - \alpha_2$ as the equality of two numbers each of

which is less than p, it cannot be divided into p. Therefore by

multiple p must be number a. But according to the condition of

theorem a it cannot be divided into p. Consequently, equality (2.12)

cannot occur.

Page 47.

In other words assumption about the fact that there is a second solution of α_2 of comparison (2.9), is invalid, and this comparison can have only unique solution among numbers of sequence (2.3).

Theorem 2.2. (Fermat low theorem). If number a is not multiple p, then with simple p is correct the comparison

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\,p). \qquad (2.13)$$

Proof. Actually/really, α_1, α_2, ..., α_{p-1} number of sequence (2.3) such, that

$$a \equiv \alpha_1 \,(\mathrm{mod}\,p), \; 2a \equiv \alpha_2 \,(\mathrm{mod}\,p), \ldots, (p-1)a \equiv \alpha_{p-1} \,(\mathrm{mod}\,p).$$

After multiplying all these comparisons with each other in accordance with the established/installed above rules, we will obtain

$$1 \cdot 2 \cdot 3 \ldots (p-1)\, a^{p-1} \equiv \alpha_1 \alpha_2 \ldots \alpha_{p-1} \,(\mathrm{mod}\,p). \qquad (2.14)$$

Let us establish/install first of all, that among numbers x_1, α_2, ..., α_{p-1} cannot be two identical numbers.

Actually/really, if we assume the presence of two identical numbers $\alpha_i = \alpha_j = c$, then this it means that occur the comparisons

$$ak_i \equiv c \,(\mathrm{mod}\,p) \; \text{и} \; ak_j \equiv c \,(\mathrm{mod}\,p),$$

i.e. that the comparison

$$ax + b \equiv 0 \,(\mathrm{mod}\,p)$$

it has two solutions k_i and k_j among numbers of sequence (2.8),
what be it cannot on the basis of corollary of the previous.
Consequently, among numbers α_1, α_2, ..., α_{p-1} cannot be identical
numbers. Let us further note that among them there is no number,
equal to zero $\alpha_i = 0$, since in this case must occur comparison
$ak_i \equiv 0 \pmod{p}$, from which it would follow that a is multiple p, and this
contradicts theorem condition.

Thus, number α_1, α_2, ..., α_{p-1} - different numbers of sequence
(2.8), moreover among them there is no zero, whence it follows that

$$\alpha_1 \alpha_2 \ldots \alpha_{p-1} = 1 \cdot 2 \cdot 3 \ldots (p-1) = (p-1)!$$

After shortening both parts of comparison (2.14) to multiplier $(p-1)!$
we will obtain (2.13) that also it is the assertion of theorem.

Let us give illustrating Fermat theorem an example.

Example. Let us take a=13, p=5. Number $a^{p-1} - 1 = 13^4 - 1 = 28561 - 1 = 28560$
is divided by 5.

Page 48.

Euler generalized Fermat theorem to the case of mutually prime

with p numbers in the following manner.

Theorem 2.3. (Euler's theorem). If number a is mutually prime
with p number, then is correct the comparison

$$a^{\varphi(p)} \equiv 1 \,(\mathrm{mod}\, p), \qquad (2.15)$$

where through $\varphi(p)$ is marked a quantity of numbers of sequence (2.8)
mutually simple ones with p, i.e., the not having with p
general/common/total cofactors.

Proof. $k_1,\ k_2,\ \ldots,\ k_{\varphi(p)}$ - mutually prime with p numbers among
numbers of sequence (2.8), and $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_{\varphi(p)}$ - number of the same
sequence, determined by the comparisons:

$$\begin{aligned}
ak_1 &\equiv \alpha_1 \,(\mathrm{mod}\, p), \qquad (2.16)\\
ak_2 &\equiv \alpha_2 \,(\mathrm{mod}\, p),\\
&\cdots\cdots\cdots\cdots\\
ak_{\varphi(p)} &\equiv \alpha_{\varphi(p)} \,(\mathrm{mod}\, p).
\end{aligned}$$

The multiplication of these comparisons leads to the comparison

$$k_1 k_2 \ldots k_{\varphi(p)} a^{\varphi(p)} \equiv \alpha_1 \alpha_2 \ldots \alpha_{\varphi(p)} \,(\mathrm{mod}\, p).$$

Let us first of all note that numbers α_i must be mutually simple
with p.

Actually/really, let us assume contrary that α_i has with p the
common factor, i.e., if p=ms, then $\alpha_i = mt$, where m, s and t -
integers.

Let us rewrite the appropriate comparison of (2.16) in the form.

$$ak_i \equiv mt \pmod{ms}$$

or in the form of the equivalent equality

$$ak_i = Lms + mt = m(Ls + t).$$

From the latter/last comparison it follows that ak_i must be divided into m. But neither a, nor k_i in view of the absence in then of general/common/total cofactors with p can be divided into m, and, therefore cannot be divided into m and their product. This shows the groundlessness of assumption about presence α_i of mutually simple with p. Further, by the already described in the previous theorem form it is established that among numbers α_i there are no identical ones.

Page 49.

Since a quantity of numbers α_i is equal to $\phi(p)$, then the sequence of the numbers

$$\alpha_1, \alpha_2, \ldots, \alpha_{\phi(p)} \qquad (2.17)$$

is the set of all numbers, mutually simple with p from sequence (2.8), in other words sequence (2.17) completely coincides (with an accuracy to sequence) with set $k_1, k_2, \ldots, k_{\phi(p)}$. Hence it follows that $k_1 k_2 \ldots k_{\phi(p)} = \alpha_1 \alpha_2 \ldots \alpha_{\phi(p)}$, that also it proves (2.15).

Example. Let us take a=5 with p=12. Let us compute $\phi(12)$. Let

us write out sequence (2.8) for p=12:1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
11. Are here emphasized the numbers of sequence, mutually simple with
12. Such numbers it proved to be 3, i.e., $\phi(12)=3$. Consequently, must
occur comparison $5^3 \equiv 1 \pmod{12}$. Testing $5^3-1=125-1=124$ (it is divided
by 12) shows the validity of this comparison.

§2.3. Primitive roots and the methods of their calculation.

Let us now move on to the examination of some
concrete/specific/actual means of comparisons.

Theorem 2.4. To the comparison
$$a^x \equiv b \pmod{p}, \qquad (2.18)$$
where p - simple, and a - mutually prime with b number, satisfies
number $x=\xi$.

Then the same comparison satisfies any number z, congruent with
ξ in modulus/module p-1, i.e.
$$z \equiv \xi \pmod{p-1}. \qquad (2.19)$$

Proof. Actually/really, if has place (2.19), then
$$z-\xi = k(p-1)$$
and, therefore, $a^{z-\xi} = a^{k(p-1)}.$

But according to Fermat low theorem
$$a^{p-1} \equiv 1 \pmod{p}.$$

which imply

$$a^{z-\xi} \equiv 1 \,(\mathrm{mod}\, p),$$

and since

$$a^{\xi} \equiv b \,(\mathrm{mod}\, p),$$

we obtain

$$a^{z} \equiv b \,(\mathrm{mod}\, p),$$

that also proves the assertion of theorem.

Page 50.

From that presented it is evident that if comparison (2.19) satisfies one number a_i of sequence (2.8), then it satisfies an infinite quantity of numbers, congruent with a_i in modulus/module $p-1$. Entire this set of the solutions, generated by number a_i, we will make as one decision. Specifically, in this sense we will indicate that comparison (2.18) has as many solutions of m, as numbers $\xi_1, \xi_2, \ldots, \xi_m$ from sequence (2.8) it satisfies.

Theorem 2.5. If the comparison

$$a^{x} \equiv 1 \,(\mathrm{mod}\, p) \qquad\qquad (2.20)$$

satisfies certain number ξ, then this comparison satisfies number $k\xi$, where k - integer.

Proof. According to theorem condition is correct the comparison

$$a^\varepsilon \equiv 1 \pmod{p}.$$

After multiplying this comparison auto to itself k of times, we will obtain the comparison

$$\underbrace{a^\varepsilon a^\varepsilon \dots a^\varepsilon}_{k \text{ раз}} \equiv 1 \pmod{p} \text{ or } a^{k\varepsilon} \equiv 1 \pmod{p},$$

constituting the assertion of theorem.

Earlier it was shown (Fermat low theorem), which comparison (2.20) always satisfies number p-1.

In general/common/total the case comparison (2.20) can have, depending on values of a and p, most varied number of solutions. In that special case when a and p are such, that the comparison has only one solution $\varepsilon = p-1$, number a is called primitive root of number p.

Far not any number p has primitive roots. In exactly the same manner there are no formulas (with exception some p of special form for which this formula they are established/installed in P. L. Chebyshev's works), which expressed the value of primitive roots in the case when it exists depending on p. The determination of primitive roots is carried out in the overwhelming majority of the

cases by simple the countershaft of numbers of sequence (2.6).

Let us consider an example of the determination of primitive roots.

Example. To find the primitive roots of number p=7.

According to Fermat theorem comparison (2.13) satisfies x=6.

Test of number a=2•2^1≡2 (mod 7); 2^2≡4 (mod 7), 2^3≡1 (mod 7); 2^4≡2 (mod 7); 2^5≡4 (mod 7); 2^6≡1 (mod 7), i.e., comparison $2^x \equiv 1 \pmod{7}$ has a solution of x=3 besides x=6. Consequently, 2 it is not primitive root.

Page 51.

Testing number a=3•3^1≡3 (mod 7); 3^2≡2 (mod 7); 3^3≡6 (mod 7); 3^4≡4 (mod 7); 3^5≡5 (mod 7); 3^6≡1 (mod 7). Thus only 6 satisfy comparison $3^x \equiv 1 \pmod{7}$, etc,3 are primitive root of number 7.

Testing number a=4•1^1≡4 (mod 7), 4^2≡2 (mod 7); 4^3≡1 (mod 7); 4^4≡4 (mod 7); 4^5≡2 (mod 7); 4^6≡1 (mod 7); x=3 is the solution of comparison $4^x \equiv 1 \pmod{7}$ besides number x=6. Number 4 is not primitive root of number 7.

Testing number a=5, $5^1 \equiv 5$ (mod 7); $5^2 \equiv 4$ (mod 7); $5^3 \equiv 6$ (mod 7); $5^4 \equiv 2$ (mod 7); $5^5 \equiv 3$ (mod 7); $5^6 \equiv 1$ (mod 7). Comparison $5^x \equiv 1$ (mod 7) has the unique solution of x=6. Consequently, 5 - primitive roots of number 7.

Testing number a=6 • $6^1 \equiv 6$ (mod 7); $6^2 \equiv 1$ (mod 7); $6^3 \equiv 6$ (mod 7); $6^3 \equiv 1$ (mod 7); $6^4 \equiv 1$ (mod 7); $6^5 \equiv 6$ (mod 7); $6^6 \equiv 1$ (mod 7). It is obvious, 6 it is not primitive roots of number 7.

By the tests conducted we computed all primitive roots of number 7, namely, 3 and 5.

Theorem 2.6. If comparison $a^x \equiv 1$ (mod p) with p simple and a nonmultiple p satisfies a number ξ, then it satisfies number d, which is the greatest common divisor of numbers ξ and p-1.

Proof. For the proof of theorem let us establish/install the following facts. If d - greatest common divisor of numbers ξ and p-1, then number A=ξ/d and B=p-1/d - mutually prime numbers. Further, if r<p and mutually simple with p, then for any m<p there is such $k_m < p$, that

$$k_m r \equiv m \,(\text{mod } p). \qquad (2.21)$$

Actually/really, in the sequence

$$r, 2r, \ldots, k_1 r, \ldots, k_2 r, \ldots, (p-1) r \qquad (2.22)$$

there are no such numbers k_1 and k_2 so that simultaneously would be performed the comparisons

$$k_1 r \equiv m \pmod{p}; \ k_2 r \equiv m \pmod{p}.$$

If both comparisons were performed, then must be performed the comparison

$$(k_1 - k_2) r \equiv 0 \pmod{p}.$$

But this is impossible, since $k_1 - k_2$ is not divided into p and r relatively prime with p.

Page 52.

Consequently, for each of (p-1) the numbers of sequence (2.22) is satisfied the comparison

$$k_i r \equiv i \pmod{p}$$

for different numbers i, where i=1, 2, ..., m, ..., p-1, and among them is $K_m r$, for which is satisfied comparison (2.21). From the established fact it follows that if A and B - two mutually prime numbers, then always it is possible to select two such numbers s and t, that

$$sA - tB = 1.$$

Actually/really, since A and B is mutually simple, then, after assuming A<B, it is possible on the basis (2.21) to write

$$sA \equiv m \pmod{B}.$$

Transition to the equality, equivalent to this comparison gives

$$sA = tB + m,$$

which correctly for any m, in particular for m=1. Thus, occurs the equality

$$s\frac{\xi}{d} - t\frac{p-1}{d} = 1$$

or

$$s\xi - t(p-1) = d.$$

From the initial comparison or theorem it follows

$$a^{s\xi} \equiv 1 \,(\text{mod}\, p),$$
$$a^{t(p-1)} \equiv 1 \,(\text{mod}\, p),$$

but after the division of the first comparison into the second we come to the comparison

$$a^{d} \equiv 1 \,(\text{mod}\, p),$$

constituting the assertion of theorem.

This theorem it is easy to spread also to the general case: if ξ and η - any two solutions of the comparison

$$a^{x} \equiv 1 \,(\text{mod}\, p),$$

where p - prime number and a is not multiple p, then this comparison satisfies their greatest common divisor.

Theorem 2.7. x - small number, which satisfies comparison

$$a^{x} \equiv 1 \,(\text{mod}\, p)$$

with simple p and a, nonmultiple p. Then α is the divider/denominator of number p-1 and all remaining numbers, which satisfy initial comparison, are multiple α.

Page 53.

Proof. ε - any solution of this comparison. According to the previous theorem this comparison it must satisfy the greatest common divisor of numbers α and ε. But in this case must be d$\leqslant\alpha$. meanwhile α - small from the numbers, which satisfy this comparison, and inequality d$<\alpha$ is impossible. Therefore, d$=\alpha$, i.e., is the divider/denominator of any solution of comparison, including p-1.

Theorem 2.8. If to the comparison
$$a^x \equiv A \,(\text{mod}\,p).\qquad(2.23)$$
where p - prime number and A is mutually simple with a, satisfies a number β, and a number α - small, that satisfies the comparison
$$a^x \equiv 1\,(\text{mod}\,p),$$
then initial comparison they satisfy p-1/α numbers, namely:
$$x \equiv \beta\,(\text{mod}\,p-1);\; x \equiv \beta + \alpha\,(\text{mod}\,p-1);$$
$$x \equiv \beta + 2\alpha\,(\text{mod}\,p-1);\ldots\qquad(2.24)$$
$$x \equiv \left[\beta + \left(\tfrac{p-1}{\alpha}-1\right)\alpha\right]\,(\text{mod}\,p-1).$$

Proof. On the basis of theorem conditions, it is possible to write the comparisons
$$a^\beta \equiv A\,(\text{mod}\,p),$$
$$a^{n\alpha} \equiv 1\,(\text{mod}\,p),$$

where n - integer.

After multiplying these comparisons, we will obtain

$$a^{\beta - n\alpha} \equiv A \pmod{p}.$$

i.e. a number $\beta + n\alpha$ with any n satisfies comparison (2.23).

General formula for x can be registered in the form

$$x = \beta + n\alpha. \qquad (2.25)$$

According to the previously proved theorem, if comparison satisfies any number β, then it satisfies any number, congruent with β in modulus/module p-1. In other words the sequence of numbers, which is obtained from (2.25) at different possible values of n, must consist of the numbers, congruent between themselves in modulus/module p-1.

Page 54.

Since x - divider/denominator p-t, then in the sequence indicated will be obtained the numbers, congruent between themselves in modulus/module p-1, when different value n are congruent between themselves in module p-1/α. Let n_i and n_j be two such values n. Then occurs the comparison

or

$$\beta + n_i\alpha \equiv \beta + n_j\alpha \pmod{p-1}$$

$$n_i\alpha \equiv n_j\alpha \pmod{p-1}.$$

Here, after shortening comparison on α, we will obtain

$$n_i \equiv n_j \left(\mathrm{mod}\,\frac{p-1}{\alpha}\right).$$

But in modulus/module $p-1/\alpha$ all numbers are congruent with any of the following numbers

$$0,\ 1,\ 2\ldots,\ \frac{p-1}{\alpha}-1.$$

Consequently, all solutions of comparison (2.23) will be congruent in module $p-1$ with any of the numbers

$$\beta,\ \beta+\alpha,\ \beta+2\alpha,\ \ldots,\ \beta+\left(\frac{p-1}{\alpha}-1\right)\alpha,$$

that also is claimed in the theorem.

To the more efficient algorithm of the determination of primitive roots, rather than testing all possible bases/bases, can give the following theorem.

Theorem 2.9. $\pi_1,\ \pi_2,\ \ldots,\ \pi_r$ - simple dividers/denominators of number $p-1$. Then the necessary and sufficient condition of the fact that q is primitive roots of the prime number p, is the nonfulfillment not of one of the comparisons

$$q^{\frac{p-1}{\pi_1}} \equiv 1 \pmod{p},\quad q^{\frac{p-1}{\pi_2}} \equiv 1 \pmod{p},\quad\ldots,\quad q^{\frac{p-1}{\pi_r}} \equiv 1 \pmod{p}.$$

$$(2.26)$$

Proof. The need for this condition is obvious, since the execution at least of one of these comparisons would indicate that

MICROCOPY RESOLUTION TEST CHART
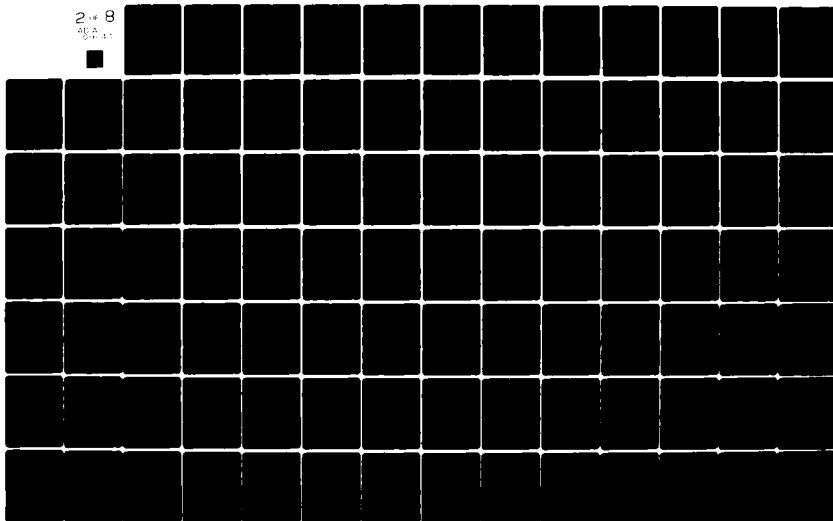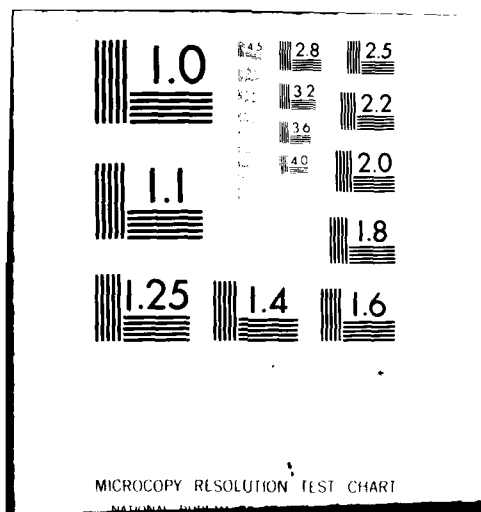
the comparison

$$q^x \equiv 1 \,(\mathrm{mod}\,p)$$

has a solution besides x=p-1 which contradicts the determination of primitive roots.

Page 55.

Let us show now the sufficiency of these conditions. Let us assume that besides solution of x=p-1 there is even some solution of the comparison

$$q^x \equiv 1 \,(\mathrm{mod}\,p)$$

x=ξ, moreover ξ<p-1 and at the same time it coincides not with one of the exponents with q, which figure in (2.26). If this solution is small, then it must divide p-1

$$\mu = \frac{p-1}{\xi}.$$

If μ - prime number, then $\mu = \pi_i$ and, therefore,

$$\xi = \frac{p-1}{\pi_i},$$

i.e. ξ is solution of one of comparisons (2.26) which contradicts the done assumption.

If μ - not simple divider/denominator of number p-1, then it can be represented in the form

$$\mu = \pi_i \vartheta,$$

where π_i - simple divider/denominator of number p-1, and

$$\xi\vartheta = \frac{p-1}{\pi_i}.$$

The assumption that ε is the solution of comparison (2.20), imply the execution of the comparison

$$q^{\varepsilon \phi} = q^{\frac{p-1}{\pi_i}} \equiv 1 \,(\text{mod } p),$$

and again we come to the contradiction.

If $\varepsilon < p-1$ - any solution of the comparison

$$q^{\varepsilon} \equiv 1 \,(\text{mod } p),$$

then there is a small solution $\alpha < p-1$ which divides ε $(\varepsilon = \alpha t)$, moreover for α is performed compulsorily one of comparisons (2.26), which is shown above. Conceal by form, and in this case we arrived at the contradiction.

Consequently, assumption $\varepsilon < p-1$ is inadmissible and comparison (2.20) can have only one solution of $x = p-1$, i.e., q is primitive roots of number p. From this theorem it follows that for calculating the primitive roots it is necessary to test/experience bases/bases only to the nonfulfillment of conditions (2.26).

Page 56.

Example. To compute primitive roots of number p=7.

Here p-1=6. The simple dividers/denominators p-1 are $\pi_1=2$, $\pi_2=3$. The system of comparisons (2.26) takes form $q^2\equiv 1$ (mod 7), $q^3\equiv 1$ (mod 7).

Test of basis/base a=2. $2^2\equiv 4$ (mod 7); $2^3\equiv 1$ (mod 7). 2 it is not primitive roots of number 7.

Testing basis/base a=3. $3^2\equiv 2$ (mod 7); $3^3\equiv 6$ (mod 7). 3 - primitive roots of number 7.

Testing basis/base a=4. $4^2\equiv 2$ (mod 7); $4^3\equiv 1$ (mod 7). 4 it is not primitive roots of number 7.

Testing basis/base a=5. $5^2\equiv 4$ (mod 7); $5^3\equiv 6$ (mod 7). 5 - primitive roots of number 7.

Testing basis/base a=6. $6^2\equiv 1$ (mod 7); $6^3\equiv 6$ (mod 7). 6 it is not primitive roots of number 7.

Thus, relying on this theorem, we obtain primitive roots of number 7 by simpler method than it is earlier.

§2.4. theory of indices.

Theorem 2.10. If q - primitive roots of number p, then the comparison

$$q^x \equiv A \pmod{p}, \qquad (2.27)$$

where A - is not multiple p, has one and only one solution.

Proof. According to the determination of primitive roots for the comparison

$$q^x \equiv 1 \pmod{p}$$

the small value x, it satisfying, exists x=p-1. Comparison (2.27) can have only one solution, since $\frac{p-1}{\alpha} - 1 = \frac{p-1}{p-1} - 1 = 0,$ or to not at all have not one solution. Theorem claims what solution is to eat. Consequently, the proof of theorem is reduced to the proof of the fact that comparison (2.27) cannot but have a solution.

Let us assume that (2.27) it does not have the solution. Since A on condition not multiply p, the A during the division into p gives in the remainder/residue any of numbers

$$1, 2, \ldots, p-1. \qquad (2.28)$$

Let this be number r, i.e.

$$A \equiv r \pmod{p}.$$

Page 57.

Then we obtain the comparison

$$q^x \equiv r \pmod{p}, \qquad (2.29)$$

which also does not have a solution, since otherwise would have the

solution and (2.27). However, since q - mutually prime with p number,
the

$$q^0, q^1, q^2, \ldots, q^{n-2}$$

is not divisible by p and, therefore, each of them in modulus/module

p is congruent with one of numbers (2.28). Hence it follows that each

of p-1 numbers

$$0, 1, 2, \ldots p-2 \qquad (2.30)$$

satisfies any of the comparisons

$$q^x \equiv 1 \,(\mathrm{mod}\, p), \; q^x \equiv 2 \,(\mathrm{mod}\, p), \; \ldots \qquad (2.31)$$
$$\ldots, \; q^x \equiv p-1 \,(\mathrm{mod}\, p).$$

Meanwhile some one of them is comparison (2.29), which, by

hypothesis, does not have a solution. Consequently, each of p-1

numbers (2.30) must satisfy any of p-2 comparisons (2.31), i.e., at

least any one of them they must satisfy two numbers of (2.30). In

other words must exist this comparison

$$q^x \equiv \rho \,(\mathrm{mod}\, p),$$

which has two solutions. But this is impossible, since earlier it was

shown that if comparison (2.27) has a solution, the only one.

Consequently, comparison (2.29) is obligated to have a solution, and

with it has the solution and comparison (2.27).

Determination. Number $\mathcal{J}$, which is the solution of the

comparison

$$q^x \equiv A \,(\mathrm{mod}\, p),$$

is called the index of number A and is designated $J = \text{ind } A$. Primitive roots q is called the basis/base of index.

From all that has been previously stated, it follows that for the determination of the index of any number A from modulus/module p it is necessary to find primitive roots of p and then to find the solution of this comparison for this primitive root.

Let us give an example of the calculation of the indices of numbers, using in this case the calculated in the previous paragraph primitive roots.

Example. To compute indices according to module 7 numbers 0, 1, 2, 3, 4, 5, 6. Primitive roots of number 7 are 3 and 5.

Let us take basis/base q=3. Let us compute 3^x for x=0, 1, 2, 3, 4, 5, 6. $3^0 \equiv 1 \pmod 7$; $3^1 \equiv 3 \pmod 7$; $3^2 \equiv 2 \pmod 7$; $3^3 \equiv 6 \pmod 7$; $3^4 \equiv 4 \pmod 7$; $3^5 \equiv 5 \pmod 7$; $3^6 \equiv 1 \pmod 7$.

Page 58.

From these comparisons it follows: ind 1=0; ind 2=2; ind 3=1; ind 4=4; ind 5=5; ind 6=3.

Let us analogously find the indices of these numbers from basis/base 5: ind 1=0; ind 2=4; ind 3=5; ind 4=2; ind 5=1; ind 6=3.

Let us establish/install new some properties of indices, which are determining the possibility of their use in the machine arithmetic, during the representation of numbers in the system of residual classes.

Theorem 2.11. If
$$A_1, A_2, \ldots, A_k$$

are positive integer numbers whose indices on modulus/module p with primitive roots of q are respectively equal to
$$i_1, i_2, \ldots, i_k,$$
and if through $\mathcal{J}$ is designated the index of the product of these numbers
$$A = A_1 A_2 \ldots A_k$$

on the modulus/module p with the same primitive roots of q, then the index of product is equal to the sum of the indices of multipliers, undertaken on modulus/module p-1, i.e.
$$\mathcal{J} = \sum_{j=1}^{k} i_j \pmod{p-1}. \tag{2.32}$$

Proof. In accordance with the determination of indices occur the comparisons
$$q^{i_1} \equiv A_1 \pmod{p}, \quad q^{i_2} \equiv A_2 \pmod{p}, \quad \ldots, \quad q^{i_k} \equiv A_k \pmod{p}.$$

After multiplying these comparisons, we will obtain
$$q^{i_1 + i_2 + \cdots + i_k} \equiv A \pmod{p}$$

or, taking into account introduced index $\mathcal{J}$ of number A,

$$q^{i_1+i_2+\dots+i_k} \equiv q^{\mathcal{J}} \,(\operatorname{mod} p).$$

Dividing

Both parts of the comparison on $q^{\mathcal{J}}$, we will obtain the comparison

$$q^{i_1+i_2+\dots+i_k-\mathcal{J}} \equiv 1 \,(\operatorname{mod} p). \qquad (2.33)$$

Since q - primitive roots of number p, then all solutions of comparison (2.33) will be multiple p-1. In other words

$$i_1+i_2+\dots+i_k-\mathcal{J} \equiv 0 \,(\operatorname{mod} p-1).$$

This comparison can be rewritten in the form (2.32).

Page 59.

In the expanded/scanned form the proved comparison can be registered as follows:

$$\operatorname{ind}(A_1 A_2 \dots A_k) \equiv \sum \operatorname{ind} A_j \,(\operatorname{mod} p-1). \qquad (2.34)$$

In other words the index of product is equal the sum of the indices of multiplier on modulus/module p-1.

§2.5. Use/application of indices for executing the arithmetic operations.

The examined in the previous section special feature/peculiarity

of indices will bring together them with the logarithms and it makes
it possible to substitute the multiplication of numbers and raising
to the power by the addition of their indices with the subsequent
transition from the index of product and degree to the product itself
and the degree. For the transition from the index to an actual number
they are applied anti-index.

Determination. The anti-index of number $\mathcal{I}$ is called number
such, that

$$\mathcal{I} = \operatorname{ind} a \quad \text{or} \quad a = \operatorname{ind}^{-1}\mathcal{I}. \qquad (2.35)$$

If anti-index is designated through $N(\mathcal{I})$, then from (2.35) it follows

$$N(\operatorname{ind} a) = a. \qquad (2.36)$$

In order to have the capability to use for purposes of multiplication
relationship/ratio (2.32), it is necessary to compute the
anti-indices of numbers. This easily is reached, as soon as there are
calculated indices of numbers, by the appropriate rotation/access of
the table of indices on the basis of expression (2.36).

Example. To compute anti-indices according to the modulus/module
of 7 numbers 0, 1, 2, 3, 4, 5.

In the previous example are given the indices of numbers from 1
to 6. Their values prove to be in the limits of sequence 0, 1, 2, 3,
4, 5. It is logical that number 0 cannot have final index, since

there is no this exponent, after raising into which final, different from zero, basis/base it would be possible to obtain 0.

Primitive roots of 3. $N(0)=1$; $N(1)=3$; $N(2)=2$; $N(3)=6$; $N(4)=4$; $N(5)=5$.

Primitive root of 5. $N(0)=1$; $N(1)=5$; $N(2)=4$; $N(3)=6$; $N(4)=2$; $N(5)=3$.

Relationship/ratio (2.34) can be used, also, for execution of division on the modulus/module. Under the division on modulus/module a/b (mod p) is understood the quotient $a+kp/b$, where k - small from the possible numbers, which convert $a+kp$ into a number, multiple b. In this case, if a/b (mod p) $=c$,

$$(\text{ind } a - \text{ind } b)(\text{mod } p-1) = \text{ind } c. \qquad (2.37)$$

Page 60.

By the use/application of indices it is possible to compute the more complicated expressions, which include the operations of multiplication, raising to the power, divisions.

Example. To compute the expression
$$c = \frac{ab^3}{k^2d} \pmod{p}.$$
where $a=2$; $b=5$; $k=3$; $d=4$; $p=7$.

1. We find indices of values, entering computed expression,
after taking primitive roots of 5: ind 2=4; ind 5=1; ind 3=5; ind
4=2.

2. We compute index of result

$$\text{ind } c \equiv 4+3-10-2 \,(\text{mod } 6), \quad \text{ind } c = 1.$$

3. We find anti-index 1: N(1)=5. Direct calculation shows that

$$c = \frac{2 \cdot 5^3}{3^2 \cdot 4} \,(\text{mod } 7) = 5.$$

§2.6. Table of indices for the simple bases/bases.

In the system of residual classes it is proposed to apply
indices for obtaining the digits of the product of numbers with each
of the bases/bases individually. Although the theory of indices can
be used also for the complicated moduli/modules and formula (2.34)
can during the proper selection of the complicated modulus/module,
which ensures the presence of primitive roots, occur for the
multiplied numbers as a whole however for the formulated target of
the use/application of indices it suffices to examine index
separately on the moduli/modules - the basis of the selected system.
In this case it is not difficult to select these bases/bases by such
that for them the primitive roots would exist and, therefore, could

be constructed the tables of indices. For any simple modulus/module the primitive roots always exists, and therefore, if we as the basis of system use prime numbers (that, generally speaking, it is appropriate and in other respects), then is satisfied both the basic requirement of the uniqueness of the representation of numbers - mutual simplicity of the basis of system and the condition for existence of primitive roots and, therefore, the possibility of the construction of the corresponding tables of indices.

Page 61.

Further are given the tables of indices for the prime numbers, written/recorded not more than by six bits. Since for the circuit realization one or another the character of the connections, which reflect tabular conformity, can prove to be more acceptable, let us give the tables of indices for some primitive roots, although is realized it must be for each basis/base the table only on any one primitive roots.

(1) Основание $p=3$
(2) индексы

q \ J	2
0	—
1	0
2	1

(1) Основание $p=5$
(2) индексы

q \ J	2	3
0	—	—
1	0	0
2	1	3
3	3	1
4	2	2

(1) Основание $p=7$
(2) индексы

q \ J	3	5
0	—	—
1	0	0
2	2	4
3	1	5
4	4	2
5	5	1
6	3	3

(1) Основание $p=11$
(2) индексы

q \ J	2	6	7	8
0	—	—	—	—
1	0	0	0	0
2	1	9	3	7
3	8	2	4	6
4	2	8	6	4
5	4	6	2	8
6	9	1	7	3
7	7	3	1	9
8	3	7	9	1
9	6	5	8	2
10	5	5	5	5

(1) Основание $p=13$
(2) индексы

q \ J	2	6	7	11
0	—	—	—	—
1	0	0	0	0
2	1	5	11	7
3	4	8	8	4
4	2	10	10	2
5	9	9	3	3
6	5	1	7	11
7	11	7	1	5
8	3	3	9	9
9	8	4	4	8
10	10	2	2	10
11	7	11	5	1
12	6	6	6	6

Key: (1). Basis/base. (2). Indices.

Page 62.

(1) Основание $p=17$
(2) индексы

q / J	3	5	6	7	10	11	12	14
0	—	—	—	—	—	—	—	—
1	0	0	0	0	0	0	0	0
2	14	6	2	10	10	2	6	14
3	1	13	15	3	11	7	5	9
4	12	12	4	4	4	4	12	12
5	5	1	11	15	7	3	9	13
6	13	3	1	13	5	9	11	7
7	11	15	5	1	9	13	7	3
8	10	2	6	14	14	6	2	10
9	2	10	14	6	6	14	10	2
10	3	7	13	9	1	5	15	11
11	7	11	9	5	13	1	3	15
12	13	9	3	7	15	11	1	5
13	4	4	12	12	12	12	4	4
14	9	5	7	11	3	15	13	1
15	6	14	10	2	2	10	14	6
16	8	8	8	8	8	8	8	8

(1) Основание $p=19$
(2) индексы

q / J	2	3	10	13	14	15
0	—	—	—	—	—	—
1	0	0	0	0	0	0
2	1	7	17	11	13	5
3	13	1	5	17	7	11
4	2	14	16	4	8	10
5	16	4	2	14	10	8
6	14	2	4	10	2	16
7	6	6	12	12	6	12
8	3	3	15	15	3	15
9	8	2	10	16	14	4
10	15	11	1	7	5	13
11	12	12	6	6	12	6
12	15	15	3	3	15	3
13	5	17	13	1	11	7
14	7	13	11	5	1	17
15	...	...	...	...	17	1
16	4	10	14	8	16	2
17	10	16	8	2	4	14
18	9	9	9	9	9	9

Key: (1). Basis/base. (2). Indices.

Page 63.

(1) Основание $p = 23$

(2) индексы

q / J	5	7	10	11	14	15	17	19	20	21
0	—	—	—	—	—	—	—	—	—	—
1	0	0	0	0	0	0	0	0	0	0
2	2	14	8	10	20	4	16	6	18	12
3	16	2	20	14	6	10	18	4	12	8
4	4	6	16	20	18	8	10	12	14	2
5	1	7	15	5	21	13	19	3	9	17
6	18	16	6	2	4	14	12	10	8	20
7	19	1	21	7	3	5	9	13	17	15
8	6	20	2	8	16	12	4	18	10	14
9	10	4	18	6	12	20	14	8	2	16
10	3	21	1	15	19	17	13	9	5	7
11	9	19	3	1	13	7	17	5	15	21
12	20	8	14	12	2	18	6	16	4	10
13	14	10	12	4	8	6	2	20	16	18
14	21	15	7	17	1	9	3	19	13	5
15	17	9	13	10	5	1	15	7	21	3
16	8	12	10	18	14	16	20	2	6	4
17	7	5	17	13	15	3	1	21	19	9
18	12	18	4	6	10	2	8	14	20	6
19	15	17	5	9	7	19	21	1	3	13
20	5	13	9	3	17	21	7	15	1	19
21	13	3	19	21	9	15	5	17	7	1
22	11	11	11	11	11	11	11	11	11	11

Key: (1). Basis/base. (2). Indices.

Основание $p=29$
индексы

q / J	2	3	8	10	11	14	15	18	19	21	26	27
0	—	—	—	—	—	—	—	—	—	—	—	—
1	0	0	0	0	0	0	0	0	0	0	0	0
2	1	17	19	11	9	13	27	23	25	5	3	15
3	5	1	11	27	17	9	23	3	13	25	15	19
4	2	6	10	22	18	26	26	18	22	10	6	2
5	22	10	26	18	2	6	6	2	18	26	10	22
6	6	18	2	10	26	22	22	26	10	2	18	6
7	12	8	4	20	24	16	16	24	20	4	8	12
8	3	23	1	5	27	11	25	13	19	15	9	17
9	10	2	22	26	6	18	18	6	26	22	2	10
10	23	27	17	1	11	19	5	25	15	3	13	9
11	25	5	27	23	1	17	3	15	9	13	19	11
12	7	7	21	21	7	7	21	21	7	7	21	21
13	18	26	6	2	22	10	10	22	2	6	26	18
14	13	25	23	3	5	1	15	19	17	9	11	27
15	27	11	9	17	19	15	1	5	3	23	25	13
16	4	12	20	16	8	24	24	8	16	20	12	4
17	21	21	7	7	21	21	7	7	21	21	7	7
18	11	19	13	9	15	3	17	1	23	27	5	25
19	9	13	3	15	25	5	19	11	1	17	27	23
20	24	16	8	12	20	4	4	20	12	8	16	24
21	17	9	15	19	13	25	11	27	5	1	23	3
22	26	22	18	6	10	2	2	10	6	18	22	26
23	20	4	16	24	12	8	8	12	24	16	4	20
24	8	24	12	4	16	20	20	16	4	12	24	8
25	16	20	14	8	4	12	12	4	8	24	20	16
26	19	15	25	13	3	23	9	17	27	11	1	5
27	15	3	5	25	23	27	13	9	11	19	17	1
28	14	14	14	14	14	14	14	14	14	14	14	14

Key: (1). Basis/base. (2). Indices.

Page 64.

(1) Основание $p=31$
(2) индексы

γ \ q	3	11	12	13	17	21	22	24
0	—	—	—	—	—	—	—	—
1	0	0	0	0	0	0	0	0
2	24	18	6	24	12	6	12	18
3	1	17	19	11	13	29	23	7
4	18	6	12	18	24	12	24	6
5	20	10	20	10	20	10	10	20
6	25	5	25	5	25	5	5	25
7	28	26	22	8	4	2	14	16
8	12	24	18	12	6	18	6	24
9	2	4	8	22	26	28	16	14
10	14	28	26	4	2	16	22	8
11	23	1	17	13	29	7	19	11
12	19	23	1	29	7	11	17	13
13	11	7	29	1	23	19	13	17
14	22	14	28	2	16	8	26	4
15	21	27	9	21	3	9	3	27
16	6	12	24	6	18	24	18	12
17	7	29	13	17	1	23	11	19
18	26	22	14	16	8	4	28	2
19	4	8	16	14	22	26	2	28
20	8	16	2	28	14	22	4	26
21	29	13	11	19	17	1	7	23
22	17	19	23	7	11	13	1	29
23	27	9	3	27	21	3	21	9
24	13	11	7	23	19	17	29	1
25	10	20	10	20	10	20	20	10
26	5	25	5	25	5	25	25	5
27	3	21	27	3	9	27	9	21
28	16	2	4	26	28	14	8	22
29	9	3	21	9	27	21	27	3
30	15	15	15	15	15	15	15	15

Key: (1). Basis/base. (2). Indices.

Page 65.
(1)Основание $p=37$
(2)Индексы

y \ q	2	5	13	15	17	18	19	20	22	24	32
0	—	—	—	—	—	—	—	—	—	—	—
1	0	0	0	0	0	0	0	0	0	0	0
2	1	11	23	25	31	17	35	13	7	5	29
3	26	34	22	2	14	10	10	14	2	22	34
4	2	22	10	14	26	34	34	26	14	10	22
5	23	2	25	35	29	31	13	11	17	7	19
6	27	9	9	27	9	27	9	27	9	27	27
7	32	28	16	8	20	4	4	20	8	16	28
8	3	33	33	3	21	15	33	3	21	15	15
9	16	32	8	4	28	20	20	28	4	8	32
10	24	12	12	24	24	12	12	24	24	12	12
11	30	6	6	30	30	6	6	30	30	6	6
12	28	20	32	16	4	8	8	4	16	32	20
13	11	13	1	23	17	7	25	35	5	19	31
14	33	3	3	33	15	21	3	33	15	21	21
15	13	35	11	1	7	5	23	25	19	29	17
16	4	8	20	28	16	32	32	16	28	20	8
17	7	5	17	31	1	11	29	19	13	35	23
18	17	7	31	29	23	1	19	5	11	13	25
19	35	25	13	11	5	19	1	23	29	31	7
20	25	23	35	13	19	29	11	1	31	17	5
21	22	26	2	10	34	14	14	34	10	2	26
22	31	17	29	19	25	23	5	7	1	11	35
23	15	21	21	15	33	3	21	15	33	3	3
24	29	31	19	5	35	25	7	17	23	1	13
25	10	2	14	34	22	26	26	22	34	14	2
26	12	24	24	12	12	24	24	12	12	14	24
27	6	30	30	6	6	30	30	6	6	30	30
28	34	14	26	22	10	2	2	10	22	26	14
29	21	15	15	21	3	33	15	21	3	33	33
30	14	10	34	26	2	22	22	2	26	34	10
31	9	27	27	9	27	9	27	9	27	9	9
32	5	19	7	17	11	13	31	29	35	25	1
33	20	4	28	32	8	16	16	8	32	28	4
34	8	16	4	20	32	28	28	32	20	4	16
35	19	29	5	7	13	35	17	31	25	23	11
36	18	18	18	18	18	18	18	18	18	18	18

Key: (1). Basis/base. (2). Indices.

Page 66.

(1) Основание $p=41$

(2) Индексы

γ \ q	6	7	11	12	13	15	17	19	22	24	26	28	29	30	34	35
0	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	26	14	22	38	6	38	2	34	34	33	38	6	38	22	14	26
3	15	25	5	5	25	35	15	15	35	35	15	5	25	25	5	35
4	12	28	4	36	12	36	4	28	28	4	36	12	36	4	28	12
5	22	18	34	26	2	6	14	38	38	14	6	2	26	34	18	22
6	1	39	27	3	31	13	17	9	29	37	33	11	23	7	19	21
7	32	1	13	37	9	27	23	31	11	3	7	29	17	33	21	19
8	38	2	26	34	18	14	6	22	22	6	14	18	34	26	2	38
9	30	10	10	10	10	30	30	30	30	30	30	10	10	10	10	30
10	8	32	16	24	8	24	16	32	32	16	24	8	24	16	32	8
11	3	37	1	9	13	39	11	27	7	31	19	33	29	21	17	23
12	27	13	9	1	37	31	19	3	23	39	11	17	21	29	33	7
13	31	9	37	13	1	3	7	39	19	27	23	21	33	17	29	11
14	25	15	35	23	15	5	25	25	5	5	25	35	15	15	35	5
15	37	3	39	31	27	1	29	13	33	9	21	7	11	19	23	17
16	24	16	8	32	24	32	8	16	16	8	32	24	32	8	16	24
17	33	7	11	7	23	29	1	17	37	21	9	3	39	31	27	13
18	16	24	32	8	16	8	32	24	24	32	8	16	8	32	24	16
19	9	31	3	27	39	37	33	1	21	13	17	19	7	23	11	29
20	34	6	38	22	14	2	18	26	26	18	2	14	22	38	6	34
21	14	26	18	2	34	22	38	6	6	38	22	34	2	18	25	14
22	29	11	23	7	19	17	13	21	1	33	37	39	27	3	31	9
23	36	4	12	28	36	28	12	4	4	12	28	36	28	12	4	36
24	13	12	31	27	3	9	21	37	17	1	29	23	19	11	7	39
25	4	36	28	12	4	12	28	36	36	28	12	4	12	28	36	4
26	17	23	19	17	7	21	9	33	13	29	1	27	31	39	3	37
27	5	35	15	15	35	25	5	5	25	25	5	15	35	35	15	25
28	11	29	17	33	21	23	27	19	39	7	3	1	13	37	9	31
29	7	33	29	21	17	11	39	23	3	19	31	37	1	9	13	27
30	23	26	21	29	33	19	31	7	27	11	39	13	9	1	37	3
31	28	12	36	4	28	4	36	12	12	36	4	28	4	36	12	28
32	10	30	30	30	30	10	10	10	10	10	10	30	30	30	30	10
33	18	22	6	14	38	34	26	2	2	26	34	38	14	6	22	18
34	19	21	33	17	29	7	3	11	31	23	27	9	37	13	1	39
35	21	19	7	23	11	33	37	29	9	17	13	31	3	27	39	1
36	2	38	14	6	22	26	34	18	18	34	26	22	6	14	38	2
37	32	8	24	16	32	16	24	8	8	24	16	32	16	24	8	32
38	35	5	25	25	5	15	35	35	15	15	35	25	5	5	25	15
39	6	34	2	18	26	18	22	14	14	22	18	26	18	2	34	6
40	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20

Key: (1). Basis/base. (2). Indices.

Pages 67-68.

(1) Основание $p = 43$

(2) индексы

γ \ q	3	5	12	18	19	20	26	28	29	30	33	34
1	0	0	0	0	0	0	0	0	0	0	0	0
2	27	33	15	27	33	3	9	39	15	33	9	3
3	1	37	13	29	31	25	5	17	41	23	19	11
4	12	24	30	12	36	6	18	36	30	24	18	6
5	25	1	31	11	19	37	41	5	17	29	13	23
6	28	28	28	14	28	28	14	14	14	14	28	14
7	35	35	35	7	35	35	7	7	7	7	35	7
8	39	15	3	39	33	9	27	33	3	15	27	9
9	2	32	26	16	20	8	10	34	40	4	38	22
10	10	34	4	38	16	40	8	2	32	20	22	26
11	30	18	12	30	6	36	24	6	12	18	24	36
12	13	19	1	41	25	31	23	11	29	5	37	17
13	32	8	28	4	26	2	34	40	10	22	20	16
14	20	26	8	34	32	38	16	4	22	40	2	10
15	26	38	2	40	8	20	4	22	16	10	32	34
16	24	6	18	24	30	12	36	30	18	6	36	12
17	38	20	32	10	2	26	22	16	4	34	8	40
18	29	23	41	1	17	11	19	31	13	37	5	25
19	19	31	37	15	1	13	11	29	23	17	25	41
20	37	25	19	23	13	1	17	41	5	11	31	29
21	36	30	6	36	24	18	12	24	6	30	12	18
22	15	9	27	15	3	39	33	3	27	9	33	39
23	16	4	40	2	34	22	38	20	26	32	10	8
24	40	10	16	26	22	34	32	8	2	38	4	20
25	8	2	20	22	38	32	40	10	34	16	26	4
26	17	41	11	31	23	5	1	37	25	13	29	19
27	3	27	39	3	9	33	15	9	39	27	15	33
28	5	17	23	19	29	41	25	1	37	31	11	13
29	41	5	29	13	11	17	37	25	1	19	23	31
30	11	29	17	25	5	23	13	19	31	1	41	37
31	34	40	22	20	4	10	2	32	8	26	16	38
32	9	39	33	9	27	15	3	27	33	39	3	15
33	31	13	25	17	37	19	29	23	11	41	1	5
34	23	11	5	37	41	29	31	13	19	25	17	1
35	18	36	24	18	12	30	6	12	24	36	6	30
36	14	14	14	28	14	14	28	28	28	28	14	28
37	7	7	7	35	7	7	35	35	35	35	7	35
38	4	22	10	32	40	16	20	26	38	8	34	2
39	33	3	9	33	15	27	39	15	9	3	39	27
40	22	16	34	8	10	4	26	38	20	2	40	32
41	6	12	36	6	18	24	30	18	36	12	30	24
42	21	21	21	21	21	21	21	21	21	21	21	21

Key: (1) Basis/base. (2) Indices

Pages 69-70.

(1)Основание p=47

(2)индексы

y \ i	5	10	11	13	15	19	20	22	23	26	29	31	33	35	38	39	40	41	43	44	45
0	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	18	30	42	10	14	28	44	32	22	26	36	6	16	34	20	8	2	38	12	40	24
3	20	18	16	6	36	26	8	10	4	34	40	22	28	2	12	14	38	32	44	24	42
4	36	14	38	20	28	10	42	18	44	6	26	12	32	22	40	16	4	30	24	34	2
5	1	17	33	21	11	45	5	35	37	27	25	31	29	7	19	3	41	43	39	15	9
6	38	2	12	16	4	8	6	42	26	14	30	28	44	36	32	22	40	24	10	18	20
7	32	38	44	28	30	14	22	16	34	36	18	26	8	40	10	4	24	42	6	20	12
8	8	44	34	30	42	38	40	4	20	32	16	18	2	10	14	24	6	22	36	28	26
9	40	36	32	12	26	6	16	20	8	22	34	44	10	4	24	28	30	18	42	2	38
10	19	1	29	31	25	27	3	21	13	7	15	37	45	41	39	11	43	35	5	9	33
11	7	27	1	9	31	39	35	15	29	5	37	33	19	3	41	21	11	25	43	13	17
12	10	32	8	26	18	36	4	28	2	40	20	34	14	24	6	30	42	16	22	12	44
13	11	3	41	1	29	35	9	17	39	21	45	19	43	31	25	33	37	13	15	27	7
14	4	22	40	38	44	42	20	2	10	16	8	32	24	28	30	12	26	34	18	14	36
15	21	35	3	27	1	25	13	45	41	15	19	7	11	9	31	17	33	29	37	39	5
16	26	28	30	40	10	20	38	36	42	12	6	24	18	44	34	32	8	14	2	22	4
17	16	42	22	14	38	30	34	8	40	18	32	36	4	20	28	2	12	44	26	10	6
18	12	20	28	22	40	34	14	6	30	2	24	4	26	38	44	36	32	10	8	42	16
19	45	29	13	25	35	1	41	11	9	19	21	15	17	39	27	43	5	3	7	31	37
20	37	31	25	41	39	9	1	7	35	33	5	43	15	29	13	19	45	27	17	3	11
21	6	10	14	34	20	40	30	26	38	24	12	2	36	42	22	18	16	28	4	44	8
22	25	11	43	19	45	21	33	1	5	31	27	39	35	37	15	29	13	17	9	7	41
23	5	39	27	13	9	41	25	37	1	43	33	17	7	35	3	15	21	31	11	29	45
24	28	16	4	36	32	18	2	14	24	20	10	40	30	12	26	38	44	8	34	6	22
25	2	34	20	42	22	44	10	24	28	8	4	16	12	14	38	6	36	40	32	30	18
26	29	33	37	11	43	17	7	3	15	1	35	25	13	19	45	41	39	5	27	21	31
27	14	8	2	18	16	32	24	30	12	10	28	20	38	6	36	42	22	4	40	26	34
28	22	6	36	2	12	24	18	34	32	42	44	38	40	16	4	20	28	26	30	8	14
29	35	43	5	45	17	11	37	29	7	25	1	27	3	15	21	13	9	33	31	19	39
30	39	19	45	37	15	1	11	31	17	41	9	13	27	43	5	25	35	21	3	33	29
31	3	5	7	17	33	43	15	13	19	35	29	1	41	21	11	9	31	37	25	45	27
32	44	12	26	4	24	2	36	22	18	38	42	30	34	32	8	40	10	6	14	16	28
33	27	45	17	15	21	19	43	25	33	39	31	9	1	5	7	35	3	11	41	37	13
34	34	26	18	24	6	12	32	40	16	44	22	42	20	8	2	10	14	36	38	4	30
35	33	9	31	3	41	13	27	5	25	17	43	11	37	1	29	7	19	39	45	35	21
36	30	4	24	32	8	16	12	38	6	38	14	10	42	26	18	44	34	2	20	36	40
37	42	24	6	8	2	4	26	44	36	30	38	14	22	18	16	34	20	12	28	32	10
38	17	13	9	35	3	29	39	43	31	45	11	21	33	27	1	5	7	41	19	25	15
39	31	21	11	7	19	15	17	27	43	9	39	41	25	33	37	1	29	45	13	5	3
40	9	15	21	5	7	37	45	39	11	13	41	3	31	17	33	27	1	19	29	43	35
41	15	25	35	39	27	31	29	19	3	37	7	5	21	13	9	45	17	1	33	41	43
42	24	40	10	44	34	22	28	12	14	4	2	8	6	30	42	26	18	20	16	38	32
43	13	37	15	43	5	33	19	41	21	29	3	35	9	45	17	39	27	7	1	11	25
44	43	41	39	29	13	3	31	33	27	11	17	45	5	25	35	37	15	9	21	1	19
45	41	7	19	33	37	5	21	9	45	3	13	29	39	11	43	31	25	15	35	17	1
46	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23

Key: (1). Basis/base. (2). Indices.

Radœs 71-72.
(1) Основание $p=53$
(2) индексы

J \ q	2	3	5	8	12	14	18	19	20	21	22	26	27	31	32	33	34	35	39	41	45	48	50	51
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	49	31	35	11	7	3	45	17	47	15	25	51	41	21	43	19	29	33	37	9	5	23	27
3	17	1	7	23	31	15	51	37	29	19	47	9	35	21	45	3	11	25	41	5	49	33	27	43
4	2	46	10	18	22	14	6	38	34	42	30	50	50	30	42	34	38	6	14	22	18	10	46	2
5	47	15	1	33	49	17	37	35	19	25	29	31	5	3	51	45	9	11	43	23	7	27	41	21
6	18	50	38	6	42	22	2	30	46	14	10	34	34	10	14	46	30	2	22	42	6	38	50	18
7	14	10	18	22	50	46	42	6	30	34	2	38	38	2	34	30	6	42	46	50	22	18	10	14
8	3	43	41	1	33	21	9	31	51	37	45	23	49	19	11	25	5	35	47	7	27	15	17	29
9	34	2	14	46	10	30	50	22	6	38	42	18	18	42	38	6	22	50	30	10	46	14	2	34
10	48	12	32	16	8	24	40	28	36	20	44	4	4	44	20	36	28	40	24	8	16	32	12	48
11	6	34	30	2	14	42	18	10	50	22	38	46	46	38	22	50	10	18	42	14	2	30	34	6
12	19	47	17	41	1	29	5	23	11	9	25	7	33	51	35	37	49	31	3	27	15	43	21	45
13	24	32	16	8	4	12	20	40	44	36	48	28	28	48	36	44	40	20	12	4	8	16	32	24
14	15	7	49	5	9	1	45	51	47	29	17	11	37	43	3	21	25	19	27	35	31	23	33	41
15	12	16	8	4	28	32	36	20	48	44	24	40	40	24	44	48	20	36	32	28	4	8	16	12
16	4	40	20	36	44	28	12	24	16	32	8	48	48	8	32	16	24	12	28	44	36	20	40	4
17	10	22	50	38	6	18	30	34	14	2	46	42	42	46	2	14	34	30	18	6	38	50	22	10
18	35	51	45	29	21	37	1	15	23	33	5	43	17	31	7	49	41	27	11	47	3	19	25	9
19	37	45	3	47	43	51	7	1	5	23	35	41	15	9	49	31	27	33	25	17	21	29	19	11
20	49	9	11	51	19	31	43	21	1	15	7	29	3	33	41	27	47	17	5	45	25	37	35	23
21	31	11	15	45	29	9	41	43	7	1	49	27	21	23	27	33	17	15	35	3	19	51	37	5
22	7	31	9	37	25	49	21	3	15	17	1	19	45	27	43	41	29	47	23	51	11	35	5	33
23	39	39	13	13	13	13	13	39	39	13	13	39	13	39	39	13	13	39	39	39	39	13	13	13
24	20	44	48	24	12	36	8	16	28	4	40	32	32	40	4	28	16	8	36	12	24	48	44	20
25	42	30	2	14	46	34	22	18	38	50	6	10	10	6	50	38	18	22	34	46	14	2	30	42
26	25	29	47	43	15	19	23	33	9	31	11	1	27	37	5	35	7	49	45	41	17	21	3	51
27	51	3	21	17	41	45	49	7	35	5	37	27	1	11	31	9	33	23	19	15	43	47	29	25
28	16	4	28	40	20	8	48	44	12	24	32	36	36	32	24	12	44	48	8	20	40	28	4	16
29	46	18	22	50	38	10	34	42	2	30	14	6	6	14	30	2	42	34	10	38	50	22	18	46
30	13	13	39	39	39	39	39	13	13	39	39	13	39	13	13	39	39	13	13	13	13	39	39	39
31	33	5	35	11	51	23	47	29	41	43	27	45	19	1	17	15	3	21	49	25	37	9	31	7
32	5	37	51	19	3	35	15	17	33	27	23	21	47	47	49	1	7	43	9	29	45	25	11	31
33	23	35	37	25	45	5	17	47	27	41	33	3	29	7	15	1	21	43	31	19	51	11	9	49
34	11	19	29	21	17	25	33	27	31	49	9	15	41	35	23	5	1	7	51	43	47	3	45	37
35	9	25	19	3	47	11	27	41	49	7	31	17	43	5	33	23	14	1	37	21	29	45	51	35
36	36	48	24	12	32	44	4	8	40	28	20	16	16	20	28	40	8	4	44	32	12	24	48	36
37	30	14	46	10	18	2	38	50	42	6	34	22	22	34	6	42	50	38	2	18	10	46	14	30
38	38	42	34	30	2	6	10	46	22	18	50	14	14	50	18	22	10	6	2	30	34	42	42	38
39	41	33	23	31	35	27	19	25	21	3	43	37	11	17	29	47	51	45	1	9	5	49	7	15
40	50	6	42	34	30	38	46	14	18	10	22	2	2	22	10	18	14	46	38	30	34	42	6	50
41	45	21	43	15	27	3	31	49	37	35	51	33	7	25	9	11	23	5	29	1	41	17	47	19
42	32	8	4	28	40	16	44	36	24	48	12	20	12	40	24	36	44	16	40	28	4	8	4	31
43	22	38	6	42	34	50	14	2	10	46	18	30	30	18	46	10	2	14	50	34	42	6	38	22
44	8	28	40	20	36	4	24	48	32	12	16	44	44	10	12	32	48	24	4	36	20	40	28	8
45	29	17	15	27	7	47	35	5	25	11	19	49	23	45	37	51	31	9	21	33	1	41	43	3
46	40	36	44	48	24	20	16	32	4	8	12	12	28	8	4	48	12	20	24	44	48	44	36	40
47	44	24	12	32	16	48	28	4	20	40	36	8	8	36	40	20	4	28	48	16	32	12	24	44
48	21	41	27	7	23	43	11	9	45	51	3	5	31	29	25	19	35	37	17	49	33	1	15	47
49	28	20	36	44	48	40	32	12	8	16	4	24	24	4	16	8	12	32	40	48	44	36	20	28
50	43	27	33	49	5	41	25	11	3	45	21	35	9	47	19	29	37	51	15	31	23	7	1	17
51	27	23	5	9	37	33	29	19	43	21	41	51	25	15	47	17	45	3	7	11	35	31	49	1
52	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26

Key: (1). Basis/base. (2). Indices.

Pages 73-74.
Основание p=59 (1)
индексы (2)

J \ q	2	6	8	10	11	13	14	18	23	24	30	31	32	33	34	37	38	39	40	42	43	44	47	50	52	52	55	56
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	33	39	25	7	49	55	27	31	23	57	45	35	41	17	19	3	11	13	37	51	43	53	9	21	5	15	47
3	50	26	36	32	2	14	24	16	42	48	8	46	10	30	38	22	34	28	12	52	56	4	40	44	6	18	54	30
4	2	8	20	50	14	40	52	54	4	46	56	32	12	24	34	38	6	22	26	16	44	28	48	18	42	10	30	36
5	6	24	2	34	42	4	40	46	12	22	52	38	36	14	44	56	18	8	20	48	16	26	28	54	10	30	32	50
6	51	1	17	57	9	5	21	43	15	13	7	33	45	3	55	41	37	39	25	31	49	47	35	53	27	23	11	19
7	18	14	6	44	10	12	4	22	36	8	40	56	50	42	16	52	54	24	22	28	48	20	26	46	30	32	38	34
8	3	41	1	17	21	31	49	23	35	11	55	19	47	7	51	57	9	33	39	53	37	13	43	27	5	15	45	25
9	42	52	14	6	4	28	48	32	26	38	16	34	20	40	18	44	10	56	24	46	54	8	22	30	12	36	50	2
10	7	57	41	1	49	53	37	15	43	45	51	25	13	55	3	17	21	19	33	27	9	11	23	5	31	35	47	39
11	25	13	47	45	1	7	41	37	21	53	33	23	5	39	19	11	17	43	35	55	57	31	49	51	3	9	27	15
12	52	34	56	24	16	54	18	12	46	36	6	20	22	44	14	2	40	50	38	10	42	32	30	4	48	28	26	8
13	45	35	15	23	25	1	39	55	3	49	13	53	9	47	11	43	19	31	5	41	33	21	7	57	17	51	37	27
14	19	47	45	11	17	3	1	49	9	31	39	43	27	25	33	13	57	35	15	7	41	5	21	55	51	37	53	23
15	54	50	38	8	44	18	6	4	54	12	2	26	46	34	24	20	52	36	32	42	14	13	10	40	16	48	28	22
16	4	16	40	42	28	22	46	50	8	34	54	6	24	48	10	18	12	44	52	32	30	56	38	36	26	20	2	14
17	10	44	52	14	48	46	54	36	22	50	18	2	8	6	42	6	4	34	56	30	10	38	32	12	28	26	20	24
18	43	27	53	31	11	19	45	1	57	3	15	21	55	23	35	5	13	9	37	25	47	51	17	39	33	41	7	49
19	38	36	32	22	34	6	2	40	18	4	20	28	54	50	8	26	56	12	30	14	24	10	42	52	44	16	48	46
20	8	32	22	26	56	44	34	42	16	10	50	12	48	38	20	36	24	30	46	6	2	54	18	14	52	40	4	28
21	10	40	42	18	12	26	28	38	20	56	48	44	2	4	54	16	30	52	14	22	46	25	8	32	36	50	34	6
22	26	46	28	12	8	56	38	6	52	18	32	10	40	22	36	30	20	54	48	34	50	16	44	2	24	14	42	4
23	15	31	5	27	47	39	13	57	1	55	43	37	3	35	23	53	45	49	21	33	11	7	41	19	25	17	51	9
24	53	9	37	49	23	45	15	39	19	1	5	7	57	27	31	21	43	3	51	47	35	17	25	13	11	33	41	55
25	12	48	4	10	26	8	22	34	24	44	46	18	14	28	30	54	36	16	40	38	32	52	56	50	20	2	6	42
26	46	10	54	48	32	50	36	24	34	14	12	40	44	30	28	4	22	42	18	20	26	6	2	8	38	56	52	16
27	34	20	50	38	6	42	14	48	10	28	24	22	30	2	56	8	44	26	36	40	52	12	4	16	18	54	46	32
28	20	22	26	36	24	52	56	18	40	54	38	30	4	8	50	32	2	16	28	44	34	48	16	16	14	42	10	12
29	28	54	48	4	22	38	32	2	56	6	30	42	52	46	12	10	26	18	16	50	36	44	34	20	8	24	14	40
30	57	25	19	33	51	9	3	31	27	35	1	13	8	17	41	39	55	47	45	21	7	15	5	49	37	53	43	11
31	49	51	55	7	53	23	27	47	11	25	9	1	33	37	21	3	31	17	57	15	5	19	45	35	43	13	39	41
32	5	49	21	9	35	13	43	19	39	57	53	51	1	31	27	37	15	55	7	11	23	41	33	45	47	25	17	3
33	17	39	25	19	3	21	7	53	5	43	41	11	15	1	57	33	51	13	47	49	55	35	31	37	9	27	23	45
34	41	19	33	39	55	37	51	5	53	15	17	47	43	57	1	25	7	45	11	9	3	23	27	21	49	31	35	13
35	24	38	8	20	52	16	44	10	48	30	34	36	28	56	2	50	14	32	22	18	6	46	54	42	40	4	12	26
36	44	2	34	56	18	10	42	28	30	26	14	8	32	6	52	24	16	20	50	4	40	36	12	48	54	46	22	38
37	55	17	57	41	37	27	9	35	23	47	3	39	11	51	7	1	49	25	19	5	21	45	15	31	53	43	13	33
38	39	11	13	47	41	55	57	9	49	27	19	15	31	33	25	45	1	23	43	51	17	53	37	3	7	21	5	35
39	37	3	51	55	27	15	5	13	45	39	21	11	19	9	49	7	53	1	17	35	31	25	47	43	23	11	33	57
40	9	7	3	51	5	35	31	11	47	33	49	57	25	21	37	55	27	41	1	43	53	39	13	23	15	45	19	17
41	14	56	24	2	40	48	16	30	28	32	44	50	26	52	6	34	42	38	8	54	18	22	46	10	4	12	36	20
42	11	15	23	43	19	17	25	7	51	21	47	31	37	45	13	35	33	5	27	1	39	9	3	41	57	55	49	53
43	33	45	11	13	57	51	17	21	37	5	25	35	53	19	39	47	41	15	23	3	1	27	9	7	55	49	31	43
44	27	21	9	37	15	47	35	33	25	41	31	35	17	5	53	49	23	7	3	13	43	1	39	11	45	19	57	51
45	48	18	16	40	46	32	30	20	38	2	10	14	56	54	4	42	28	6	44	36	12	34	50	26	22	8	24	52
46	16	6	44	52	54	30	10	26	32	20	42	24	38	18	40	14	48	2	34	12	4	50	36	28	46	22	8	56
47	23	5	27	53	45	25	47	41	17	7	35	49	51	15	43	31	11	21	9	39	13	3	1	33	19	57	55	37
48	54	42	18	16	30	36	12	8	50	24	4	52	34	10	48	40	46	14	6	26	28	2	20	22	32	38	56	44
49	36	28	12	30	20	24	8	44	14	16	22	54	42	26	32	47	50	48	4	56	38	40	52	34	2	6	18	10
50	13	23	43	35	33	57	19	3	55	9	45	5	49	11	47	15	39	27	53	17	25	37	51	1	41	7	21	31
51	32	12	30	46	50	2	20	52	6	40	26	48	18	36	22	28	38	4	10	34	8	42	14	56	34	44	16	54
52	47	43	35	15	39	41	33	51	7	37	11	27	21	13	45	23	25	53	31	57	19	49	55	18	1	3	9	5
53	22	30	46	28	38	34	50	14	44	42	36	4	16	32	26	12	8	10	54	2	20	18	6	24	56	52	40	48
54	35	53	31	5	13	33	11	17	41	51	23	9	7	43	15	27	47	37	49	19	45	55	57	25	39	1	3	21
55	31	37	49	21	43	11	23	25	33	17	27	3	41	53	5	9	35	51	55	45	15	57	19	47	13	39	1	7
56	21	35	7	3	31	43	53	45	13	19	37	17	39	49	9	51	5	57	41	23	27	33	11	15	35	47	25	1
57	30	4	10	54	36	20	26	56	2	52	28	16	6	12	46	48	32	40	42	8	22	14	24	38	50	34	44	18
58	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29	29

Key: (1). Basis/base. (2). Indices.

(1) Основание $p=61$

(2) индексы

$\diagdown$ J \ q	2	6	7	10	17	18	26	30
1	0	0	0	0	0	0	0	0
2	1	43	49	47	23	37	41	29
3	6	18	54	42	18	42	6	54
4	2	26	38	34	46	14	22	58
5	22	46	58	14	26	34	2	38
6	7	1	43	29	41	19	47	23
7	49	7	1	23	47	13	29	41
8	3	9	27	21	9	51	3	27
9	12	36	48	24	36	24	12	48
10	23	29	47	1	49	11	43	7
11	15	45	15	45	45	45	45	45
12	8	44	32	16	4	56	28	52
13	40	40	40	20	20	40	20	20
14	50	50	50	10	10	50	10	10
15	28	4	52	56	44	16	8	32
16	4	52	16	8	32	28	44	56
17	47	41	23	49	1	59	7	43
18	13	19	37	11	59	1	53	17
19	26	38	14	22	58	2	46	34
20	24	12	36	48	12	48	24	36
21	55	25	55	5	5	55	35	35
22	16	28	4	32	8	52	56	44
23	57	51	33	39	51	9	57	33
24	9	27	21	3	27	33	9	21
25	44	32	56	28	52	8	4	16
26	41	23	29	7	43	17	1	49
27	18	54	42	6	54	6	18	42
28	51	33	39	57	33	27	51	39
29	35	5	35	25	25	35	55	55
30	29	47	41	43	7	53	49	1
31	59	17	11	13	37	23	19	31
32	5	35	5	55	55	5	25	25
33	21	3	9	27	3	57	21	9
34	48	24	12	36	24	36	48	12
35	11	53	59	37	13	47	31	19
36	14	2	26	58	22	38	34	46
37	39	57	51	33	57	3	39	51
38	27	21	3	9	21	39	27	3
39	46	58	34	2	38	22	26	14
40	25	55	25	35	35	25	5	5
41	54	42	6	18	42	18	54	6
42	56	8	44	52	28	32	16	4
43	43	49	7	41	29	31	23	47
44	17	11	53	19	31	29	37	13
45	34	22	46	38	2	58	14	26
46	58	34	22	26	14	46	38	2
47	20	20	20	40	40	20	40	40
48	10	10	10	50	50	10	50	50
49	38	14	2	46	34	26	58	22
50	45	15	45	15	15	45	45	45
51	53	59	17	31	19	41	13	37
52	42	6	18	54	6	54	42	18
53	33	39	57	51	39	21	33	57
54	19	37	31	53	17	43	59	11
55	37	31	13	59	11	49	17	53
56	52	16	28	54	56	4	32	8
57	32	56	8	4	16	44	52	28
58	36	48	24	12	48	12	36	24
59	31	13	19	17	53	7	11	59
60	30	30	30	30	30	30	30	30

Key: (1). Basis/base. (2). Indices.

Page 77.

Chapter 3.

BASES OF MACHINE ARITHMETIC IN A SYSTEM OF RESIDUAL CLASSES.

§3.1. Rank of a number and its property.

Let be preset the system with bases/bases $p_1, p_2, \ldots, p_n$, range of which $\mathscr{P}$ is defined as

$$\mathscr{P} = \prod_{i=1}^{n} p_i.$$

As is known, any number A from range $(0, \mathscr{P})$ in a single manner can be represented in the form of remainders/residues on the selected mutually simple bases/bases, namely:

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n).$$

To the preset system of bases/bases unambiguously corresponds the system of the orthogonal bases

$$B_1, B_2, \ldots, B_n,$$

of such, that the value of number A in the positional numeration

system can be represented as

$$A \equiv \sum_{i=1}^{n} \alpha_i B_i \,(\text{mod } \mathcal{P}) \qquad (3.1)$$

or, which is the same,

$$A = \sum_{i=1}^{n} \alpha_i B_i - r_A \mathcal{P}, \qquad (3.2)$$

where r_A positive integer number, which shows, how often the range of system $\mathcal{P}$ was exceeded upon transfer from the representation of a number in the system of residual classes to its positional representation through the system of orthogonal bases.

Page 78.

Positive integer number r_A we will call the true rank or simply by the rank of number A.

Let us formulate the theorem about the rank of the sum of two numbers.

Theorem 3.1. (about the rank of sum). If in the system with bases/bases $p_1, p_2, \ldots, p_n$ and range $\mathcal{P}$ preset two numbers: $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, and $B = (\beta_1, \beta_2, \ldots, \beta_n)$, with ranks r_A and r_B respectively, then rank r_{A+B} of the sum of these numbers will be defined as

$$r_{A+B} = r_A + r_B - \sum_{i=1}^{n} \left[\frac{\alpha_i + \beta_i}{p_i} \right] m_i, \qquad (3.3)$$

where m_i the weight of orthogonal base B_i.

Proof. Let us write in accordance with (3.2) expressions for numbers A and B:

$$A = \sum_{i=1}^{n} \alpha_i B_i - r_A \mathcal{P},$$

$$B = \sum_{i=1}^{n} \beta_i B_i - r_B \mathcal{P}.$$

Adding A and B, we will obtain

$$A + B = \sum_{i=1}^{n} (\alpha_i + \beta_i) B_i - (r_A + r_B) \mathcal{P}, \qquad (3.4)$$

on the other hand, on the basis of the rules of the calculation of the sum of two numbers we can write

$$A + B = \left(\alpha_1 + \beta_1 - \left[\frac{\alpha_1 + \beta_1}{p_1} \right] p_1, \ldots, \alpha_n + \beta_n - \left[\frac{\alpha_n + \beta_n}{p_n} \right] p_n \right)$$

or in the form (3.2)

$$A + B = \sum_{i=1}^{n} \left(\alpha_i + \beta_i - \left[\frac{\alpha_i + \beta_i}{p_i} \right] p_i \right) B_i - r_{A+B} \mathcal{P}. \quad (3.5)$$

Page 79.

We convert this expression

$$A + B = \sum_{i=1}^{n} (\alpha_i + \beta_i) B_i - \sum_{i=1}^{n} \left[\frac{\alpha_i + \beta_i}{p_i} \right] p_i B_i - r_{A+B} \mathcal{P} =$$

$$= \sum_{i=1}^{n} (\alpha_i + \beta_i) B_i - \sum_{i=1}^{n} \left[\frac{\alpha_i + \beta_i}{p_i} \right] m_i \mathcal{P} - r_{A+B} \mathcal{P}. \quad (3.6)$$

Equalizing right sides (3.4) and (3.6), we obtain assertion (3.3) of theorem.

Obtained expression (3.3) is the fundamental principles, which makes it possible to count the rank of sum on the ranks of components/terms/addends. It is obvious that $\left[\frac{\alpha_i + \beta_i}{p_i} \right] = 1$, if $\alpha_i + \beta_i > p_i$, and $\left[\frac{\alpha_i + \beta_i}{p_i} \right] = 0$ otherwise.

Logical to assume that frequently the determination of rank will be produced directly in the process of executing the operation, being its essential part. Therefore let us consider one of the possible methods of determining the rank without the transition to the positional representation of a number. Let us designate through M_i the minimum from numbers of the form

$$(0, 0, 0 \ldots 0, t_i, t_{i+1}, \ldots, t_n).$$

Is obvious, this will be represented in the adopted system number, equal to the product of the following basis of system:

$$p_1 p_2 \ldots p_{i-1}.$$

Thus,

$$M_1 = (1, 1, \ldots, 1),$$
$$M_2 = (0, p_1, p_1, \ldots, p_1),$$
$$M_3 = (0, 0, p_1 p_2 (\mathrm{mod}\, p_3), \ldots, p_1 p_2 (\mathrm{mod}\, p_n)) \text{ and so forth.}$$

Let $A = (\alpha_1, \alpha_2 \ldots, \alpha_n)$ be the number whose rank r_A should be computed. Numbers M_i and their ranks r_i we assume/set by known ones, since they are determined only by the basis of system. We will to number A adjoin number M_1 as many times, as will be required so that the digit of number A on basis/base p_1 would become equal to zero.

Let us assume that for this was necessary k_1 times to adjoin number M_1, and as a result of addition was formed number A_1 with rank r_{A_1}

$$A_1 = A + k_1 M_1.$$

Page 80.

Then applying consecutively/serially k_1 times formula (3.3), we will obtain

$$r_{A_1} = r_A + \omega_1,$$

where ω_1 - known to us value.

Let us now move on to the second stage of procedure. Let us produce the analogous additions k_2 of times of number M_2 to number A_1 before obtaining of zero remainder/residue with basis/base p_2. In

this case we will obtain number A_2 with rank r_{A_2}:

$$A_2 = A_1 + k_2 M_2.$$

Applying consecutively/serially k_2 times formula (3.3), we will obtain

$$r_{A_2} = r_A - \omega_2.$$

where ω_2 - known to us value.

Continuing this process on all digits of a number, as a result we will obtain the number $(0, 0, ..., 0)$, equal to $\mathscr{P}$, rank of which, as can easily be seen, is equal - 1. On the other hand, the calculated rank of this number is equal to $r_A + \omega_n$, whence it follows that

$$r_A = -\omega_n - 1. \qquad (3.7)$$

Let us give the example, which illustrates the method of determining the rank of a number examined.

Let us select system of calculation with bases/bases $p_1=3$, $p_2=5$, $p_3=7$. In this case the range of system will be equal to $\mathscr{P}=3\cdot5\cdot7=105$.

The orthogonal bases of system are defined as $B_1=70$, $B_2=21$, $B_3=15$, and their weight with respect to kA $m_1=2$, $m_2=1$, $m_3=1$.

For the selected system we write the minimum numbers:

$$M_1 = (1, 1, 1), \quad M_2 = (0, 3, 3), \quad M_3 = (0, 0, 1),$$

ranks of which are equal to

$$r_1 = 1, \; r_2 = 1, \; r_3 = 0.$$

Example. To find rank r_A of number $A = (1, \; 1, \; 5) = 61$.

Let us sum number A with M_1

$$(1, 1, 5) + (1, 1, 1) = (2, 2, 6).$$

Transitions through the bases/bases it was not; therefore the rank of sum will be defined on (3.3) as

$$r = r_A + 1.$$

It is repeated the procedure indicated again

$$(2, 2, 6) + (1, 1, 1) = (0, 3, 0).$$

In this case occurred the transitions through bases/bases $p_1 = 3$, $p_3 = 7$; therefore

$$r = r_A + 1 + 1 - 2 - 1 = r_A - 1.$$

Page 81.

Let us now move on to the transition into zero digits on the second basis/base with the help of number M_2

$$(0, 3, 0) + (0, 3, 3) = (0, 1, 3).$$

In this case occurred overfilling on the second basis/base. Therefore the rank of result will be equal to

$$r = r_A - 1 + 1 - 1 = r_A - 1.$$

It is repeated the addition

$$(0, 1, 3) + (0, 3, 3) = (0, 4, 6).$$

Transitions it was not. The rank of a number will be

$$r = r_A - 1 - 1 = r_A.$$

We continue the process

$$(0, 4, 6) + (0, 3, 3) = (0, 2, 2).$$

Transition occurred through bases/bases p_2 and p_3, i.e.,

$$r = r_A - 1 - 2 = r_A - 1.$$

And, finally

$$(0, 2, 2) + (0, 3, 3) = (0, 0, 5).$$

We here have an overflow on the second basis/base

$$r = r_A - 1 + 1 - 1 = r_A - 1.$$

Let us switch over to transition into zero digits on basis/base p_3

$$(0, 0, 5) + (0, 0, 1) = (0, 0, 6).$$

Transitions it was not

$$r = r_A - 1.$$

It is repeated the addition

$$(0, 0, 6) + (0, 0, 1) = (0, 0, 0).$$

In this case

$$r = r_A - 1 - 1 = r_A - 2.$$

In accordance with (3.7) we will obtain

$$r_A - 2 = -1,$$

whence $r_A = 1$. Actually/really, the rank of number A, determined according to (3.2),

$$A = B_1 + B_2 + 5B_3 = 166 - 1 \cdot 105$$

is equal to $r_A = 1$.

The given above method of determining the rank of a number by
consecutive additions with preset minimum codes M_i can be
simplified, if we have in the storage of machine codes, multiple
minimum, and their ranks. Then it is possible to conduct the
calculation of rank by consecutive subtractions in n procedures.

Page 82.

Definition. The rank of the number, which is the result of
arithmatic operation, obtained from the ranks of operands is called
the calculated rank of a number.

It is logical that if the operation is performed correctly, then
calculated rank and true rank of result during the comparison will
prove to be identical.

As it will be proved further, the calculation of the rank of
result with the execution of the operation of addition and its
comparison with the true rank of result make it possible to
establish/install the fact of output/yield or nonappearance of result
from range $[0, \mathscr{P})$, i.e. the fact of overflow.

Let us consider some examples in the system with bases/bases $p_1=3$, $p_2=5$, $p_3=7$.

Example. To sum number $A=(1, 3, 2)=58$ rank of which $r_A=1$. with number $B=(1, 1, 2)=16$ with rank $r_B=1$. We store/add up

$$A + B = (1, 3, 2) + (1, 1, 2) = (2, 4, 4).$$

The rank of sum will be $r_{A+B}=1+1=2$. As it is easy to check, the true rank of number $(2, 4, 4)$ is equal to 2. Thus the calculated and true ranks of result coincided, therefore, overflows was not.

Example. To sum number $A=(1, 3, 2)=58$ with number $B=(1, 3, 2)=58$. Here $r_A=r_B=1$. We store/add up

$$A + B = (1, 3, 2) + (1, 3, 2) = (2, 6, 4).$$

Rank of sum $r_{A+B}=1+1-1=1$. The true rank of number $(2, 1, 4)$ is equal to 2 and does not coincide with the calculated rank, which means, occurred overflow. Is actual/real, $A+B=58+58=116>105$.

§3.2. On the expanded representation of numbers.

Until now, number A in the system of residual classes was represented in the form

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Let us introduce now the representation of a number in the form

$$A' = (\lambda_1\alpha_1 + (1-\lambda_1)(\alpha_1-p_1), \ldots, \lambda_n\alpha_n + (1-\lambda_n)(\alpha_n-p_n)),$$
$$(3.8)$$

where λ_i (i=1, 2, ..., n) can be equally either 1 or 0. Representation (3.8) subsequently we will call the expanded representation of number λ.

Ordinary representation corresponds to the case when everything $\lambda_i = 1$. If $\lambda_i = 0$, then the corresponding digit of a number will be negative. Relative to the expanded representations occurs the following theorem.

Page 83.

Theorem 3.2. In the system with bases/bases $p_1, p_2, \ldots, p_n$, by range $\mathscr{P}$ and orthogonal bases $B_1, B_2, \ldots, B_n$, with single weights of
$$m_1 = m_2 = \ldots = m_n = 1$$ for any number A by rank r_A there is an expanded representation of zero rank.

Proof. In reality, after placing
$$\lambda_{i_1} = \lambda_{i_2} = \ldots = \lambda_{i_{r_A}} = 0,$$
and others $\lambda_j = 1$, we will obtain on (3.8)
$$A' = (\alpha_1, \alpha_2, \ldots, \alpha_{i_1} - p_{i_1}, \ldots, \alpha_{i_{r_A}} - p_{i_{r_A}}, \ldots, \alpha_n).$$
Let us present this number in its disintegration in terms of the orthogonal bases
$$A' = \alpha_1 B_1 + \alpha_2 B_2 + \ldots + \alpha_{i_1} B_{i_1} + \ldots + \alpha_{i_{r_A}} B_{i_{r_A}} + \ldots + \\ + \alpha_n B_n - (p_{i_1} B_{i_1} + p_{i_2} B_{i_2} + \ldots + p_{i_{r_A}} B_{i_{r_A}}).$$

Since we selected the system of bases/bases for which $p_i B_i = \mathcal{P}$, that

$$A' = \alpha_1 B_1 + \alpha_2 B_2 + \ldots + \alpha_n B_n - r_A \mathcal{P} = A.$$

This expanded representation of a number we will name the principal expanded representation.

Corollary 1. The rank of a number is equal to a quantity of negative digits in its principal expanded representation.

Corollary 2. The maximum rank of a number does not exceed n-1 (n - order of system). This escape/ensues from the fact that all digits of principal fixed expansion cannot be negative, at least one of the digits must be positive. Thus, principal fixed expansion of a number can contain not more than n-1 negative digits.

Corollary 3. A maximally possible rank for the number, which has k of zeros, does not exceed n-k-1.

The upper limit of the value of the rank of a number can be somewhat lowered. This possibility is determined by the following theorem.

Theorem 3.3. A maximally attainable rank of number A in its principal expanded representation does not exceed n-2.

Page 84.

Proof. The proof of this theorem must consist in the demonstration of the fact that by one positive digit cannot be gathered the positive number in the principal expanded representation. In reality, let $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a number with the greatest possible rank and we found such principal expanded representation A', in which $\lambda_j = 1$, and the others

$$\lambda_i = 0,$$
$$i = 1, 2, \ldots, n, \quad i \neq j$$

Then

$$A' = \alpha_j B_j - ((p_1 - \alpha_1) B_1 + (p_2 - \alpha_2) B_2 + \ldots$$
$$\ldots + (p_{j-1} - \alpha_{j-1}) B_{j-1} + (p_{j+1} - \alpha_{j+1}) B_{j+1} + \ldots$$
$$\ldots + (p_n - \alpha_n) B_n). \qquad (3.9)$$

It is obvious, A' will be greatest, when positive components/terms/addends are greatest, and negative - smallest in the absence of zero digits, i.e.,

$$\alpha_i = p_i - 1,$$
$$i = 1, 2, \ldots, n.$$

Then

$$A' = \mathscr{P} - (B_1 + B_2 + \ldots + B_n) = \mathscr{P} - (\mathscr{P} + 1) = -1.$$

Meanwhile $A = (p_1 - 1, p_2 - 1, \ldots, p_n - 1) = \mathscr{P} - 1$ and, thus, (3.9) it is not the main thing they are expanded, by representation A. The latter will be obtained, if we preserve in A' by positive one additional digit, that also is claimed under theorem condition. Then will occur the equality

$$A' = 2\mathscr{P} - (\mathscr{P} + 1) = \mathscr{P} - 1.$$

Let us take now as the orthogonal bases of the value:

$$\begin{aligned}
B_1 &= (k_1, \ 0, \ 0, \ \ldots, 0), \\
B_2 &= (0, \ k_2, \ 0, \ \ldots, 0), \\
&\ \cdots\cdots\cdots\cdots\cdots \\
B_n &= (0, \ 0, \ 0, \ \ldots, k_n),
\end{aligned} \qquad (3.10)$$

where k_i can have values $1, 2, \ldots, p_i - 1$ for i=1, 2, ..., n.

Let in the selected system of bases/bases be is preset number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Page 85.

Let us select values $\lambda_1, \lambda_2, \ldots, \lambda_n$ in such a way that would occur the following comparisons:

$$\begin{aligned}
k_1\lambda_1 &\equiv \alpha_1 \ (\mathrm{mod}\ p_1), \\
k_2\lambda_2 &\equiv \alpha_2 \ (\mathrm{mod}\ p_2), \\
&\ \cdots\cdots\cdots\cdots \\
k_n\lambda_n &\equiv \alpha_n \ (\mathrm{mod}\ p_n)
\end{aligned} \qquad (3.11)$$

or

$$\lambda_1 \equiv \frac{\alpha_1}{k_1} \pmod{p_1}.$$
$$\cdots \cdots \cdots \qquad (3.12)$$
$$\lambda_n \equiv \frac{\alpha_n}{k_n} \pmod{p_n}.$$

Let us name the expression

$$\widetilde{A} = (\lambda_1, \lambda_2, \ldots, \lambda_n) \qquad (3.13)$$

the inverse representation of number A, and the constant value

$$K = (k_1, k_2, \ldots, k_n) \qquad (3.14)$$

- by gate of inverse representation.

Between the integers of range $[0, \mathscr{P})$ and the inverse representations of these numbers (3.13) occurs one-to-one conformity, since from (3.11), (3.13) and (3.14) we have

$$\widetilde{A}K \equiv A \pmod{\mathscr{P}}$$

or

$$\widetilde{A} \equiv \frac{A}{K} \pmod{\mathscr{P}}.$$

It is obvious that the in question, until now, representations of numbers in the form of remainders/residues on the selected bases/bases of the form

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$$

are also the inverse representations of numbers with the gate

$$K = (1, 1, \ldots, 1).$$

Since $k_i \neq 0$ (i=1, 2, ..., n), then as the gates of different inverse representations can serve $\prod_{i=1}^{n}(p_i - 1)$ different numbers of the range

$(0, \mathscr{P})$ and there is respectively as many different inverse represantations of numbers and so many the systems of orthogonal bases.

Let us agree that to negative digits $\alpha_i - p_i$ in the expanded reprasentation correspond negative digits $\lambda_i - p_i$ in the inverse representation.

Among the gates of inverse representation is a gate of the form

$$K = (1, 1, \ldots, 1).$$

This follows from (3.12) when $\alpha_i = \lambda_i.$

Page 86.

The value of gate is determined by the expression

$$K = \sum_{i=1}^{n} B_i - r_k \mathscr{P}, \qquad (3.15)$$

where r_k - rank of gate or respectively

$$K \equiv \sum_{i=1}^{n} B_i \,(\text{mod } \mathscr{P}).$$

Thus, in the system of residual classes are possible the various forms of the representation of numbers, differing by greater or smaller simplicity.

The given here expanded and inverse representations carry more complicated character, but make it possible to minimize the maximum value of true rank numbers, which in a number of cases can prove to be useful, taking into account nonmodularity of rank.

§3.3. Numerical sequences and the ranks of their elements/cells.

Let us consider some questions of distribution in interval $[0, \mathscr{P})$ of the members of the sequence

$$a_{is} = (\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, S, \alpha_{i+1}, \ldots, \alpha_n),$$
$$s = 0, 1, \ldots, p_i - 1. \qquad (3.16)$$

As can be seen from (3.16) the members of this sequence differ from each other only in terms of their digit in base p_i.

Lemma 3.1. In the system with bases/bases $p_1, p_2, \ldots, p_n$, by orthogonal bases $B_1, B_2, \ldots, B_n$, of weight of which respectively $m_1, m_2, \ldots, m_n$, and range $\mathscr{P} = \prod_{i=1}^{n} p_i$ in each of the intervals

$$\left[(j-1)\frac{\mathscr{P}}{p_i}, \; j\frac{\mathscr{P}}{p_i} \right),$$
$$j = 1, 2, \ldots, p_i, \qquad (3.17)$$

of range $\mathscr{P}$ is contained according to one number of sequence a_{is}.

Page 87.

Proof. Is actual/real, since

$$B_i = m_i \frac{\mathcal{P}}{p_i},$$

where $m_i < p_i$, that the difference between two members of sequence a_{is_1} and a_{is_2}, ranks of which are respectively equal to r_1 and r_2 will be defined as

$$a_{is_2} - a_{is_1} = (S_2 - S_1)\, m_i \frac{\mathcal{P}}{p_i} - (r_2 - r_1)\, \mathcal{P}. \qquad (3.18)$$

So that a_{is_1} and a_{is_2} would lie/rest at one interval, it is necessary that there would be such integer k, for which occurs the equality

$$(S_2 - S_1)\, m_i \frac{\mathcal{P}}{p_i} - (r_2 - r_1)\, \mathcal{P} = k\mathcal{P}, \qquad (3.19)$$

i.e. so that the value

$$l = \frac{S_2 - S_1}{p_i} m_i$$

would be integer.

Since p_i - prime number, and $m_i < p_i$ and $S_2 - S_1 < p_i$, the l cannot be integer. Consequently, equality (3.19) is impossible. This means that any two numbers of sequence (3.16) are located in different intervals (3.17). Since in all terms in sequence p_i and as many different intervals, then in each of these intervals it is contained on one member of sequence.

Corollary. Among numbers $a_{i\bullet}$ of sequence (3.16) is contained only one number $a_{i\bullet\bullet}$ such, which $p_i a_{i\bullet}$ lies/rests at interval $[0, \mathcal{P})$.

In reality, from determination $a_{i\bullet}$ in interval (3.17) follows determination $p_i a_{i\bullet}$ in interval $[(j-1)\mathcal{P}, j\mathcal{P})$.

In particular, assuming/setting $j=1$, we come to formulated in the corollary assertion.

Lemma 3.2. If one of the numbers $a_{i\bullet_1}$ with rank r_1 of the numerical sequence

$$a_{i\bullet} = (\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, S, \alpha_{i+1}, \ldots, \alpha_n),$$

where $S=0, 1, \ldots, p_i-1$, is located in the interval

$$\left[(j-1)\frac{\mathcal{P}}{p_i}, j\frac{\mathcal{P}}{p_i}\right),$$

the number $a_{i(\bullet_1+l)}$ with rank r_t, where t>0, is located in the interval

$$\left[\left(j + tm_i - 1 - \left[\frac{j+tm_i-1}{p_i}\right]p_i\right)\frac{\mathcal{P}}{p_i}, \right.$$
$$\left. \left(j+tm_i - \left[\frac{j+tm_i}{p_i}\right]p_i\right)\frac{\mathcal{P}}{p_i}\right). \qquad (3.20)$$

Page 88.

Proof. In accordance with (3.18) we can write

$$a_{i(\bullet_1+l)} = a_{i\bullet_1} + tm_i\frac{\mathcal{P}}{p_i} - (r_t - r_1)\mathcal{P}.$$

Since t>0, then the border of the interval in which is located $a_{i(s_1+l)}$, they are obtained by addition to the borders of the interval in which is located a_{is_1}, value

$$tm_i\frac{\mathscr{P}}{p_i}$$

and by the exception/elimination of a possible number of full waves (depending on values m_i), that also is reflected in (3.20).

Corollary. If member a_{is} of sequence (3.16) is situated in the interval

$$\left[(j-1)\frac{\mathscr{P}}{p_i},\ j\frac{\mathscr{P}}{p_i}\right),$$

then in the following interval

$$\left[j\frac{\mathscr{P}}{p_i},\ (j+1)\frac{\mathscr{P}}{p_i}\right)$$

is located number a_{is_i}, where

$$S_i = S + \frac{\lambda^i_{ij}p_i+1}{m_i}. \qquad (3.21)$$

Here through λ^i_{ij} is designated the integer part of the expression

$$\lambda^i_{ij} = \left[\frac{j+tm_i-1}{p_i}\right].$$

Actually/really, assuming/setting in (3.20)

$$j+1 = j+tm_i-\lambda^i_{ij}p_i,$$

we will obtain that

$$t = \frac{\lambda^i_{ij}p_i+1}{m_i}, \qquad (3.22)$$

that also proves the assertion of corollary.

From (3.22) it is evident that m_i must be the divider/denominator of value $\lambda_{tj}^i p_i + 1$. In a number of cases this can occur only at the unique value of value λ_{tj}^i. In particular, when $m_i = 1$ must be $\lambda_{tj}^i = 0$ and then t=1. In other words if $m_i = 1$, then a_{is} and $a_{i(s+1)}$ are located in the adjacent intervals.

Page 89.

Lemma 3.3. The members of numerical sequence a_{is_1} and a_{is_2} of the identical rank $r_1 = r_2 = r$ satisfy inequality $a_{is_1} < a_{is_2}$, if is satisfied the condition $S_1 < S_2$.

Proof. In accordance with the conditions of lemma expression (3.18) can be rewritten in the form

$$a_{is_2} - a_{is_1} = (S_2 - S_1) B_i,$$

i.e. with $S_2 > S_1$ we will obtain $a_{is_2} > a_{is_1}$, that also is the assertion of lemma.

Lemma 3.4. If the members of numerical sequence a_{is_1} and a_{is_2} with

ranks r_1 and r_2 respectively satisfy the inequality

$$a_{i_2} > a_{i_1},$$

then their ranks they satisfy the inequality

$$r_2 \leqslant r_1 + m_i - 1. \qquad (3.23)$$

Proof. From the condition of lemma it follows that

$$(S_2 - S_1) B_i - (r_2 - r_1) \mathscr{P} > 0$$

or

$$(S_2 - S_1) B_i > (r_2 - r_1) \mathscr{P}. \qquad (3.24)$$

Let us assume that inequality (3.23) does not occur, i.e.,

$$r_2 - r_1 > m_i - 1$$

or

$$r_2 - r_1 \geqslant m_i.$$

But then from (3.24) it follows that

$$S_2 - S_1 > p_i,$$

which is impossible. It remains to take the assertion of lemma.

Corollary 1. If $a_{i_2} > a_{i_1}$, then with single weight $m_i = 1$ of orthogonal base B_i lesser numbers have not smaller ranks: $r_2 \leqslant r_1$.

In this case the greatest rank has the smallest number, i.e., a number, which is located in interval $\left[0, \frac{\mathscr{P}}{p_i} \right)$.

Corollary 2. A difference in the ranks of any two numbers of the examined numerical sequence in the absolute value is less than the

weight m_i of the corresponding orthogonal base.

Page 90.

Theorem 3.4. If are preset the members

$$a_{i0}, a_{i1}, \ldots, a_{i(s^*-1)}, a_{is^*}, a_{i(s^*+1)}, \ldots, a_{i(p_i-1)}$$

of the numerical sequence of the form

$$a_{is} = (\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, S, \alpha_{i+1}, \ldots, \alpha_n),$$

where

$$S = 0, 1, 2, \ldots, p_i - 1.$$

and if when $m_i = 1$ a minimum number of sequence is a_{is^*} with rank r^* ,
then terms $a_{i0}, a_{i1}, \ldots a_{i(s^*-1)}$ have ranks, equal to r^*-1, and terms a_{is^*},
$a_{i(s^*+1)}, \ldots, a_{i(p_i-1)}$ have early hours they are equal to r^*.

Proof. Actually/really, since $m_i = 1$, that any numbers a_{is} and
$a_{i(s+1)}$ are located in the adjacent intervals. In other words number
$a_{i(s+1)}$ is obtained from a_{is} by the addition of the number

$$B_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0),$$

of that having zero rank.

If a_{is^*} is a minimum number of sequence with rank r^*, then it is
located in interval $\left[0, \frac{\mathscr{P}}{p_i} \right)$ and, therefore, $a_{i(s^*+1)}$ is located in
interval $\left[\frac{\mathscr{P}}{p_i}, 2\frac{\mathscr{P}}{p_i} \right)$, $a_{i(s^*+2)}$ - in interval $\left[2\frac{\mathscr{P}}{p_i}, 3\frac{\mathscr{P}}{p_i} \right)$ and so forth,
until $S^* + \rho < p_i$, all numbers

$$a_{is^*}, a_{i(s^*+1)}, \ldots, a_{i(s^*+\rho)}$$

to $\rho = p_i - S^* - 1$ are have a rank r* since they are formed by addition with number B_i of zero rank, moreover nowhere occurs transition through p_i, which it could change rank. It is a different matter when $\rho = p_i - S^*$. Number $a_{i(s^*-p_i-s^*)} = a_{i0}$ will already have a rank r*-1, since during the addition with B_i will occur the transition through p_i, which will determine decrease per unit of the rank of sum. Rank r*-1 they will have all numbers from a_{i0} to $a_{i(s^*-1)}$.

Corollary 1. If S*=0, then in the numerical sequence all numbers have identical ranks. Actually/really, in this case with the formation/education of the next members of sequence by additions B_i there is nowhere transition through p_i, in other words there is no derating that it could change rank to that or other side.

Page 91.

Further continuation of sequence with addition B_i to $a_{i(p_i-1)}$ leads to a_{i0} and it is conjugated/combined, on one hand, with derating, what increases true rank in comparison with the calculated per unit, and on the other hand - with the transition through p_i, which reduces the rank per unit. The combined action of these two factors leaves the rank of number a_{i0} without the changes.

Corollary 2. Let Σ_i indicate the sum of all members of sequence (3.16). Then during calculation Σ_i they take place $\frac{p_i-1}{2}$ of derating $(0, \mathcal{F})$.

In reality, we have

$$a_{is} = a_{i(s*+p)} = a_{is*} + \rho\,\frac{\mathcal{F}}{p_i}\ .$$

let us compute Σ_i

$$\Sigma_i = \sum_{s=0}^{p_i-1} a_{is} = \sum_{s=0}^{\nu_i-1} a_{is*} + \frac{\mathcal{F}}{p_i}\sum_{\rho=0}^{p_i-1}\rho = p_i a_{1s*} + \frac{p_i-1}{2}\,\mathcal{F}.$$

Since $p_i a_{is*}$ lies/rests in the range $(0, \mathcal{F})$, then in all during calculation Σ_i they take place $\frac{p_i-1}{2}$ of derating.

Determination. System with bases/bases $p_1, p_2, \ldots, p_n$, by range B_1, $\mathcal{F} = \prod_{i=1}^{n} p_i$, by orthogonal bases $B_2, \ldots, B_n$, of weight of which is respectively equal to $m_1, m_2, \ldots m_n$, we will call standardized/normalized on basis/base p_i, if occurs condition $m_i = 1\ (i = 1, 2, \ldots, n)$.

If system is calibrated on largest basis/base, then this system of bases/bases we will call the simply standardized/normalized system.

Theorem 3.5. If in the standardized/normalized on basis/base p_i system of bases/bases is known rank r_Σ of sum Σ_i of all members of numerical sequence, then minimum member $a_{i\ast}$ of this sequence and rank his $r\ast$ are defined as the integral solutions of the indeterminate equation

$$p_i r\ast - S\ast = r_\Sigma + \delta - \left[\frac{p_i - 1}{2}\right], \qquad (3.25)$$

where δ is determined through the total number of transitions on all bases/bases, which occur during calculation Σ_i. i.e.

$$\delta = \sum_{j=1}^{n} \left[\frac{p_i \alpha_j}{p_j}\right] m_j.$$

Page 92.

Proof. Since in the sequence in question there are by $S\ast$ of numbers of rank $r\ast - 1$ and $p_i - S\ast$ numbers of rank $r\ast$, about according to corollary of 2 3.4 to the theorem about the rank of sum we have

$$r_\Sigma = S\ast(r\ast - 1) + (p_i - S\ast) r\ast - \delta + \left[\frac{p_i - 1}{2}\right],$$

which after simplification brings to (3.25).

Observation. Since $S\ast < p_i$, the equation (3.25) has the unique integral solution, which is determining unknown $S\ast$ and $r\ast$.

Let us consider some examples for the system of the bases/bases:
$p_1=3$, $p_2=5$, $p_3=7$, the illustrating properties of numerical sequences
presented.

Example. Let sequence a_{3i} take form (2, 3, 0), (2, 3, 1), (2, 3,
2), (2, 3, 3), (2, 3, 4), (2, 3, 5), (2, 3, 6), i.e., its terms in
the value are equal to:

$$a_{30}=98; \; a_{31}=8, \; a_{32}=23, \; a_{33}=38, \; a_{34}=53, \; a_{35}=68, \; a_{36}=83.$$

and the ranks of them respectively:

$$r_{30}=1, \; r_{31}=2, \; r_{32}=2, \; r_{33}=2, \; r_{34}=2, \; r_{35}=2, \; r_{36}=2.$$

Since here $S^*=1$ that the rank of numbers from (2, 3, 1) and d
(2, 3, 6) is equal to 2, and the rank of number (2, 3, 0) is equal to
1.

Example. Let sequence a_{3i} take the form

$$(2, 4, 0), \; (2, 4, 1), \; (2, 4, 2), \; (2, 4, 3), \; (2, 4, 4), \; (2, 4, 5), \; (2, 4, 6).$$
$$a_{30}=14, \; a_{31}=29, \; a_{32}=44, \; a_{33}=59, \; a_{34}=74, \; a_{35}=89, \; a_{36}=104.$$

Here $S^*=0$ and all members of sequence have one and the same
rank, equal to 2.

Example. Is known rank r_1 of number (1, 3, 0). Number (1, 3, 0)
can be obtained as sum Σ_i of the members of sequence (1, 4, 0), (1,

4, 1), (1, 4, 2), (1, 4, 3), (1, 4, 4), (1, 4, 5), (1, 4, 6) then
equation (3.25) of signs the form

$$.7r^* - S^* = 10,$$

whence we obtain r*=2, S*=4.

Actually/really (1, 4, 4)=4 there is a small number of this
sequence and its rank is equal to 2.

Theorem 3.6. If in the standardized on basis/base p_i system with
the odd bases/bases two members $a_{i(q-1)}$ and a_{iq} of the numerical
sequence

$$a_{is} = (\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, S, \alpha_{i+1}, \ldots, \alpha_n),$$
$$S = 0, 1, \ldots, p_i - 1$$

have identical parity, then term a_{iq} is the minimum member of
sequence, i.e., q=S*.

Page 93.

Proof. Since all basis of system are odd, then is odd value

$$B_i = \frac{\mathscr{P}}{p_i}.$$

If we the rank of number $a_{i(q-1)}$ designate through r_1, and the rank of
number a_{iq} - through r_2, then according to (3.18) we have

$$a_{iq} - a_{i(q-1)} = \frac{\mathscr{P}}{p_i} - (r_2 - r_1)\,\mathscr{P}.$$

If one assumes that $r_2=r_1$ then it will seem that a difference in two numbers of identical parity is odd, which is impossible. Hence $r_2 \neq r_1$ which is possible only when $q=S*$ i.e. term a_{iq} is the minimum term of numerical sequence in question.

§3.4. Orthogonal and pseudo-orthogonal numbers.

Numbers, in which all digits zero, with exception of digit on basis/base p_i, i.e. numbers of form

$$A_i = (0,\ 0,\ \ldots,\ 0,\ \alpha_i,\ 0,\ \ldots,\ 0),\qquad (3.26)$$

we will call orthogonal on basis/base p_i numbers. During the calculation of the true rank of a number it is most logical it would be logical consider number $A = (\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n)$ as the sum of its orthogonal components, and the rank of number A to compose as the sum of the ranks of these components. However, this path does not reach target, since with the addition of orthogonal components can take place beyond the limits of range $(0,\ \mathscr{P})$, the not catched in the process additions. Specifically, these possible outputs/yields for the range substantially will influence the value of rank. Therefore it is considered by advisable to find such standard components whose ranks would be previously known so that the number A would be represented by the sum of these components and so that with the addition it would

not be outputs/yields beyond the limits of range $(0, \mathscr{P})$. It is obvious, these components must be sufficiently small.

Such standard components subsequently we will call pseudo-orthogonal numbers.

Page 94.

Determination. Pseudo-orthogonal number $\overline{A}_i$ on basis/base p_i is called such number which is obtained from orthogonal number A_i, if we in it break orthogonality on any basis/base (for example, on p_n), i.e. a number of form

$$\overline{A}_i = (0, 0, \ldots, 0, \alpha_i, 0, \ldots, 0, S_{\alpha_i}) = \alpha_i B_i + S_{\alpha_i} B_n. \quad (3.27)$$

It is possible to examine the pseudo-orthogonal numbers, in which the orthogonality is broken on any of the bases/bases; however, we subsequently for the certainty will always examine pseudo-orthogonal numbers of form (3.27). This not at all breaks the generality of examination, since by p_n can be implied any of the basis of system.

Extending property of numerical sequences to pseudo-orthogonal numbers, let us find the number

$$M_{\alpha_i} = (0, 0, \ldots, \alpha, \ldots, 0, S_{\alpha}^*), \quad (3.28)$$

lying at interval $\left[0, \frac{\mathscr{P}}{p_n}\right)$.

Such numbers subsequently we will call minimum pseudo-orthogonal numbers.

Digit $S_{x_i}^*$ on basis/base p_n, with which a pseudo-orthogonal number has minimum value, i.e., it falls into interval $\left[0, \frac{\mathscr{P}}{p_n}\right)$, we will call the trace of pseudo-orthogonal number $\overline{A}_i$. Let us generalize the concept of the trace of a number.

Let to us be is preset number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Digit S_A^* on basis/base p_n such, with which the number

$$A^* = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A^*)$$

is located in interval $\left[0, \frac{\mathscr{P}}{p_n}\right)$, will call minimum of the traces of number A.

Number A* whose digits in bases/bases p_1, p_2, ..., p_{n-1} coincide with the digits of number A, and digit on basis/base p_n is minimal trace of number A, we will call the minimum form of number A.

Let us establish/install some properties of minimum forms.

Page 95.

Theorem 3.7. If in the standardized/normalized system are represented two numbers:

$$A_1 = (\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_{n-1}^{(1)}, \alpha_n^{(1)}),$$
$$A_2 = (\alpha_1^{(2)}, \alpha_2^{(2)}, \ldots, \alpha_{n-1}^{(2)}, \alpha_n^{(2)}),$$

minimum forms of which are

$$A_1^* = (\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_{n-1}^{(1)}, S_{A_1}^*),$$
$$A_2^* = (\alpha_1^{(2)}, \alpha_2^{(2)}, \ldots, \alpha_{n-1}^{(2)}, S_{A_2}^*),$$

but the minimum form of sum $A_1^* + A_2^*$ takes the form

$$(A_1^* + A_2^*)^* = (\gamma_1, \gamma_2, \ldots, \gamma_{n-1}, S^*)$$

then the minimum trace S^* of the sum of the minimum forms of numbers A_1 and A_2 satisfies the relationship/ratio

$$S_{A_1}^* + S_{A_2}^* - 1 \,(\text{mod } p_n) \leqslant S^* \leqslant S_{A_1}^* + S_{A_2}^* \,(\text{mod } p_n). \quad (3.29)$$

Proof. Since according to the condition of theorem $m_n = 1$, then value $\dfrac{\mathscr{P}}{p_n}$ can be represented as

$$\frac{\mathscr{P}}{p_n} = q p_n - 1,$$

where q - positive integer number.

Let us present numbers A^*_1 and A^*_2 in the form

$$A_1^* = q_1 p_n + S_{A_1}^*,$$
$$A_2^* = q_2 p_n + S_{A_2}^*,$$

where q_1 and q_2 - whole non-negative numbers.

Then on the strength of the fact that A^*_1 and A^*_2 are minimum forms, occur the inequalities

$$q_1 < q,$$
$$q_2 < q,$$

indicating the determination of numbers $A*_1$ and $A*_2$ in interval

$$\left[0, \frac{\mathscr{P}}{p_n}\right].$$

Sum $A*_1$ and $A*_2$ can be presented in the form

$$A_1^* + A_2^* = \left(q_1 + q_2 + \left[\frac{S_{A_1}^* + S_{A_2}^*}{p_n}\right]\right) p_n + (S_{A_1}^* + S_{A_2}^*) \pmod{p_n}.$$

let us consider the possible relationships/ratios between sum of $q_1 + q_2$ and value q.

Case 1.

At this case sum $A*_1 + A*_2$ lies/rests at interval $\left[0, \frac{\mathscr{P}}{p_n}\right]$, i.e. it is minimum and, therefore,

$$(S_{A_1}^* + S_{A_2}^*) \pmod{p_n} = S^*.$$

Page 96.

Case of 2. $q_1 + q_2 + \left[\frac{S_{A_1}^* + S_{A_2}^*}{p_n}\right] > q.$

At this case sum $A*_1 + A*_2$ lies/rests at interval $\left[\frac{\mathscr{P}}{p_n}, 2\frac{\mathscr{P}}{p_n}\right]$, i.e. the minimum form of sum $A*_1 + A*_2$ differs from value $A*_1 + A*_2$ by value $\mathscr{P}/p_n$, i.e.

$$(A_1^* + A_2^*)^* = A_1^* + A_2^* - \frac{\mathcal{P}}{p_n} =$$
$$= \left(q_1 + q_2 + \left[\frac{S_{A_1}^* + S_{A_2}^*}{p_n} \right] - q \right) p_n +$$
$$\div (S_{A_1}^* + S_{A_2}^* - 1) \, (\text{mod} \, p_n).$$

Whence

$$(S_{A_1}^* + S_{A_2}^* - 1) \, (\text{mod} \, p_n) = S^*.$$

Both the cases examined are reflected in relationship/ratio (3.29).

The obtained result can be spread to any number of components/terms/addends, for which let us formulate more general/more common/more total theorem.

Theorem 3.3. If in the standardized/normalized system are represented numbers $A_1, \ldots, A_m$, minimum forms of which are

$$\dot{A}_1^* = (\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_{n-1}^{(1)}, S_{A_1}^*),$$
$$A_2^* = (\alpha_1^{(2)}, \alpha_2^{(2)}, \ldots, \alpha_{n-1}^{(2)}, S_{A_2}^*),$$
$$\cdots \cdots \cdots \cdots \cdots \cdots \cdots$$
$$A_m^* = (\alpha_1^{(m)}, \alpha_2^{(m)}, \ldots, \alpha_{n-1}^{(m)}, S_{A_m}^*),$$

and if the minimum form of sum $\sum\limits_{i=1}^{m} A_i^*$ takes the form

$$\left(\sum_{i=1}^{m} A_i^* \right)^* = (\gamma_1, \gamma_2, \ldots, \gamma_{n-1}, S_\Sigma^*),$$

the minimum trace of the sum of minimum forms satisfies the

relationship/ratio

$$\sum_{i=1}^{m} S_{A_i}^{*} - m + 1 \pmod{p_n} \leqslant S_{\Sigma}^{*} \leqslant \sum_{i=1}^{m} S_{A_i}^{*} \pmod{p_n}. \quad (3.30)$$

Theorem is proven (m-1) by the --fold use/application of previous theorem 3.7.

Let us consider some theorems about traces and ranks of minimum pseudo-orthogonal numbers.

Page 97.

Theorem 3.9. If in the standardized/normalized system is preset the minimum pseudo-orthogonal number

$$M_{\alpha_i} = (0, 0, \ldots, \alpha_i, \ldots, 0, S_{\alpha_i}^{*})$$

with rank r_{α_i}, then its trace $S_{\alpha_i}^{*}$ is defined as

$$S_{\alpha_i}^{*} = \left[\frac{(r_{\alpha_i} p_i - \alpha_i m_i) p_n}{p_i} \right] + 1. \quad (3.31)$$

Proof. The value of minimum pseudo-orthogonal number M_{α_i} can be registered in the form

$$M_{\alpha_i} = \alpha_i B_i + S_{\alpha_i}^{*} B_n - r_{\alpha_i} \mathcal{P}.$$

In accordance with the determination of a minimum pseudo-orthogonal number, M_{α_i} is located in interval $\left[0, \frac{\mathcal{P}}{p_n} \right)$, i.e.

$$0 \leqslant M_{\alpha_i} < \frac{\mathcal{P}}{p_n}$$

or

$$r_{\alpha_i}\mathscr{P} < \alpha_i m_i \frac{\mathscr{P}}{p_i} + S^*_{\alpha_i} \frac{\mathscr{P}}{p_n} < r_{\alpha_i}\mathscr{P} + \frac{\mathscr{P}}{p_n},$$

whence

$$\frac{(r_{\alpha_i} p_i - \alpha_i m_i)\, p_n}{p_i} \leqslant S^*_{\alpha_i} < \frac{(r_{\alpha_i} p_i - \alpha_i m_i)\, p_n}{p_i} + 1.$$

Since $S^*_{\alpha_i}$ - numerical number, then it can satisfy the obtained inequality only at the value

$$S^*_{\alpha_i} = \left[\frac{(r_{\alpha_i} p_i - \alpha_i m_i)\, p_n}{p_i} \right] + 1,$$

that also is the assertion of theorem.

Theorem 3.10. If in the standardized/normalized system is preset the minimum pseudo-orthogonal number

$$M_{\alpha_i} = (0, 0, \ldots, \alpha_i, \ldots, 0, S^*_{\alpha_i}),$$

then its rank r_{α_i} I determines by the expression

$$r_{\alpha_i} = \left[\frac{\alpha_i m_i}{p_i} \right] + 1. \qquad (3.32)$$

Page 98.

Proof. From expression (3.31) for $S^*_{\alpha_i}$ it follows, on one hand, that

$$r_{\alpha_i} p_i - \alpha_i m_i > 0,$$

i.e.

$$r_{\alpha_i} > \frac{\alpha_i m_i}{p_i}, \qquad (3.33)$$

and on the other hand, since $S_{\alpha_i}^* < p_n$,

$$r_{\alpha_i} p_i - \alpha_i m_i < p_i,$$

i.e.

$$r_{\alpha_i} < \frac{\alpha_i m_i}{p_i} + 1. \qquad (3.34)$$

Since r_{α_i} - whole, then the only possibility to satisfy simultaneously relationships/ratios (3.33) and (3.34) is execution (3.32).

Corollary. A minimum pseudo-orthogonal number with digit α_i, to equal unity, has single rank.

Actually/really, since $\left[\frac{m_i}{p_i}\right] = 0$, that $r_{\alpha_i} = 1$. Theorem 3.11. If in the standardized/normalized system is preset the minimum pseudo-orthogonal number

$$M_{\alpha_i} = (0, 0, \ldots, \alpha_i, \ldots, 0, S_{\alpha_i}^*)$$

with rank r_{α_i} and the minimum pseudo-orthogonal number

$$M_{p_i - \alpha_i} = (0, 0, \ldots, p_i - \alpha_i, \ldots, 0, S_{p_i - \alpha_i}^*),$$

with rank $r_{p_i - \alpha_i}$, then the ranks of these minimum pseudo-orthogonal numbers are connected with the relationship/ratio

$$r_{\alpha_i} + r_{p_i - \alpha_i} = m_i + 1, \qquad (3.35)$$

and their traces satisfy the relationship/ratio

$$S_{\alpha_i}^* + S_{p_i - \alpha_i}^* = p_n + 1. \qquad (3.36)$$

Proof. Let us count the sum of the ranks of numbers M_{α_i} and $M_{p_i - \alpha_i}$:

$$r_{\alpha_i} + r_{p_i-\alpha_i} = \left[\frac{\alpha_i m_i}{p_i}\right] + 1 + \left[\frac{(p_i-\alpha_i) m_i}{p_i}\right] + 1 =$$
$$= \left[\frac{\alpha_i m_i}{p_i}\right] + \left[-\frac{\alpha_i m_i}{p_i}\right] + m_i + 2.$$

In accordance with the fact that the integer part [x] of the fractional number x satisfies the relationship/ratio

$$[x] + [-x] = -1,$$

we will obtain

$$r_{\alpha_i} + r_{p_i-\alpha_i} = m_i + 1.$$

Page 99.

Let us count now the sum of the traces of $q_1 + q_2 + \left[\frac{S^*_{A_1} + S^*_{A_2}}{p_n}\right] < q.$ pseudo-orthogonal numbers in accordance with (3.31):

$$S^*_{\alpha_i} + S^*_{p_i-\alpha_i} = \left[\frac{(r_{\alpha_i} p_i - \alpha_i m_i) p_n}{p_i}\right] + 1 +$$
$$+ \left[\frac{(r_{p_i-\alpha_i} p_i - (p_i-\alpha_i) m_i) p_n}{p_i}\right] + 1 = p_n + 1.$$

Corollary. If $\alpha_i = 1$, the minimum pseudo-orthogonal number M_{p_i-1} for the further digit on basis/base p_i has a rank, equal to m_i.

Is actual/real, on (3.35) $r_{p_i-1} = m_i.$

Example. Let us consider the system of the bases/bases:

$$p_1 = 2, \ p_2 = 5, \ p_3 = 7, \ p_4 = 23. \ \mathscr{P} = 1610,$$

let us count orthogonal bases and their weights

$$B_1 = \frac{1610}{2} = 805; \qquad m_1 = 1,$$

$$B_2 = \frac{3 \cdot 1610}{5} = 966; \qquad m_2 = 3,$$

$$B_3 = \frac{6 \cdot 1610}{7} = 1380; \qquad m_3 = 6,$$

$$B_4 = \frac{1610}{23} = 70; \qquad m_4 = 1.$$

For the adopted system let us give the values of minimum pseudo-orthogonal numbers and their ranks:

on basis/base $p_1 = 2$

$$(1, 0, 0, S^*_{\alpha_1}) = (1, 0, 0, 12) = 35, \ r_1 = 1;$$

on basis/base $p_2 = 5$

$$(0, 1, 0, S^*_{\alpha_2}) = (0, 1, 0, 10) = 56, \ r_1 = 1,$$
$$(0, 2, 0, S^*_{\alpha_2}) = (0, 2, 0, 19) = 42, \ r_2 = 2,$$
$$(0, 3, 0, S^*_{\alpha_2}) = (0, 3, 0, 5) = 28, \ r_3 = 2,$$
$$(0, 4, 0, S^*_{\alpha_2}) = (0, 4, 0, 14) = 14, \ r_4 = 2;$$

on basis/base $p_3 = 7$

$$(0, 0, 1, S^*_{\alpha_3}) = (0, 0, 1, 4) = 50, \ r_1 = 1,$$
$$(0, 0, 2, S^*_{\alpha_3}) = (0, 0, 2, 7) = 30, \ r_2 = 2,$$
$$(0, 0, 3, S^*_{\alpha_3}) = (0, 0, 3, 10) = 10, \ r_3 = 3,$$
$$(0, 0, 4, S^*_{\alpha_3}) = (0, 0, 4, 14) = 60, \ r_4 = 4,$$
$$(0, 0, 5, S^*_{\alpha_3}) = (0, 0, 5, 17) = 40, \ r_5 = 5,$$
$$(0, 0, 6, S^*_{\alpha_3}) = (0, 0, 6, 20) = 20, \ r_6 = 6.$$

Page 100.

Here values $S_{\alpha_i}^*$ and r_{α_i} were calculated respectively according to formulas (3.31) and (3.32). Values of minimum pseudo-orthogonal numbers as this is clearly evident, they lie/rest into the range

$$\left[0, \frac{\mathscr{P}}{p_n}\right) = [0, 70).$$

§3.5. Composition of a number of the minimum pseudo-orthogonal components.

Let us consider in that calibrated in the standardized/normalized system certain number

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n).$$

Summarizing the minimum pseudo-orthogonal numbers

$$M_{\alpha_1}, M_{\alpha_2}, \ldots, M_{\alpha_{n-1}},$$

we form number M_A:

$$M_A = M_{\alpha_1} + M_{\alpha_2} + \ldots + M_{\alpha_{n-1}}$$

or

$$M_A = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A),$$

where

$$S_A = (S_{\alpha_1}^* + S_{\alpha_2}^* + \ldots + S_{\alpha_{n-1}}^*) \,(\bmod \, p_n). \qquad (3.37)$$

Value S_A subsequently we will call the trace of a number A.

As is evident number M_A, differs from number A only in terms of digit in the latter/last basis/base.

Since each of the components/terms/addends lies/rests, regarding, in the range $\left[0, \frac{\mathscr{P}}{p_n}\right)$, i.e.

$$M_{\alpha_1} < \frac{\mathscr{P}}{p_n} - 1,$$

then after $(n-1)$ addition we obtain

$$M_A \leqslant (n-1)\left(\frac{\mathscr{P}}{p_n} - 1\right).$$

Under condition $p_n > n-1$ we obtain $M_A < \mathscr{P}$, i.e. with formation/education M_A is ensured nonappearance for range $[0, \mathscr{P})$.

The true rank of obtained number M_A to us it is always accurately known, since the true rank coincides with the calculated if the sum stays in the range.

Page 101.

However, calculated rank, as is known, is defined according to the theorem about the addition of ranks as the sum of the ranks of operands minus the sum of the allowed transitions through the value of basis/base taking into account their weights.

Since on all digits, except digit on the latter/last foundation for, transitions with the addition of minimum pseudo-orthogonal numbers being it cannot, but the weight of orthogonal base on the latter/last basis/base was accepted equal to unity, this circumstance substantially simplifies the calculation of the rank of a number.

Let us designate through K_A the sum of the ranks of the minimum pseudo-orthogonal numbers

$$K_A = \sum_{i=1}^{n-1} r_{\alpha_i} \qquad (3.38)$$

and we will subsequently of number K_A call the kernel of the rank of number A.

Let us designate through π_A a number of transitions on the latter/last basis/base, which occurred with the performed addition

$$\pi_A = \left[\frac{S^\circ_{\alpha_1} + S^\circ_{\alpha_2} + \ldots + S^\circ_{\alpha_{n-1}}}{p_n} \right], \qquad (3.39)$$

and we will subsequently number π_A call the correction of the rank of number A.

Then the true rank of number M_A is defined as

$$r_{M_A} = K_A - \pi_A. \qquad (3.40)$$

Thus, minimum pseudo-orthogonal numbers serve as the convenient

standard components by summarizing which it is possible to obtain the number, which coincides with any initial number in all digits, except digit by the latter/last basis/base. In this case to us is known the rank of the obtained number.

According to (3.30) the minimum trace of sum S_A^* is connected with the trace of number A with the relationship/ratio

$$S_A - n + 2 \leqslant S_A^* \leqslant S_A. \qquad (3.41)$$

The inequality can be refined by considering the number of zeros among the digits of the number A: $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$.

After designating a quantity of zero digits through ω_A it is possible to rewrite (3.41) in the form

$$S_A - n + 2 + \omega_A \leqslant S_A^* \leqslant S_A. \qquad (3.42)$$

Page 102.

From (3.40) we know the true rank of number M_A, meanwhile as it interests the true rank of number A.

In a number of cases it can be determined immediately, depending on the relationship/ratio between α_n and S_A. Let us formulate the theorem, which is determining, when the rank of number A can be determined immediately according to the rank of number M_A.

Theorem 3.12. If in the standardized/normalized system of the number

$$A(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n)$$

and by the addition of the minimum pseudo-orthogonal numbers

$$M_{\alpha_1}, M_{\alpha_2}, \ldots, M_{\alpha_{n-1}}$$

obtained is number $M_A = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A)$ with rank r_{M_A}, then rank r_A of number A is preset determined by the expression

$$r_A = r_{M_A} - \Delta_A. \qquad (3.43)$$

where Δ_A can have a value $\Delta_A = 0, 1, -1$.

Proof. From the properties of numerical sequences it is known that the members of the sequence of the form

$$(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S),$$

whose value S are equal to $S_A^*, S_A^* + 1, \ldots, p_n - 1$, they have a rank, per unit larger than the terms which have $S = 0, 1, 2, \ldots S_A^* - 1$. Hence, knowing the rank of number M_A and examining different mutual locations of zero on basic/base p_n, α_n, S_A^* and S_A, we will obtain values r_A, equal to r_{M_A}, greater r_{M_A} per unit and smaller r_{M_A} per unit.

Let us consider different possible cases:

Case 1. If zero through basis/base p_n are located out of interval $(S_A - n + 2 + \omega, S_A)$, which is equivalent to the condition

then
$$S_A - n + 2 + \omega > 0,$$
$$r_A = r_{M_A} \text{ при } \alpha_n \geqslant S_A \qquad (I)$$
and
$$r_A = r_{M_A} - 1 \text{ при } \alpha_n < S_A - n + 2 + \omega. \qquad (I')$$

Key: (1). with.

Case of 2. If zero on basis/base p_n are arranged/located within segment $(S_A - n + 2 + \omega, S_A)$ but is more left S_A^*, that to condition $S_A^* > 0$, then equivalent occurs the same relationship

$$r_A = r_{M_A} \quad \text{при} \quad \alpha_n \geqslant S_A,$$
$$r_A = r_{M_A} - 1 \quad \text{при} \quad \alpha_n < S_A^*.$$

Key: (1). with.

Page 103.

Case of 3. If $S_A^* = 0$, then from the properties of numerical sequences to us it is known that $r_A = r_{M_A}$ for any α_n,

Case of 4. If zero on basis/base p_n are arranged/located within segment (S_A^*, S_A) or it coincides with its right border $S_A = 0$, then,

and
$$r_A = r_{M_A} + 1 \quad \text{для} \quad \alpha_n \geqslant S_A^*$$
$$r_A = r_{M_A} \quad \text{для} \quad \alpha_n < S_A^*.$$

that also proves the assertion of theorem. Key: (1). for.

Thus, if is known rank r_{M_A} of number M_A, then for determining the

rank of the arbitrary number A it is necessary to know the mutual relationship/ratio of values α_n, S_A^*, S_A and zero on basis/base p_n, i.e. the rank of number A coincides with the rank of number M_A if

and
$$\alpha_n \geqslant S_A^* \overset{(1)}{\text{и}} S_A \geqslant S_A^*$$
$$\alpha_n < S_A^* \overset{(1)}{\text{и}} S_A < S_A^*.$$

Key: (1). and.

The rank of number A per unit is more than the rank of number M_A

if
$$r_A = r_{M_A} + 1,$$
$$\alpha_n \geqslant S_A^* \overset{(1)}{\text{и}} S_A < S_A^*.$$

Key: (1). and.

The rank of number A per unit is less than the rank of number M_A

if
$$r_A = r_{M_A} - 1,$$
$$\alpha_n < S_A^* \overset{(1)}{\text{и}} S_A \geqslant S_A^*.$$

Key: (1). and.

On the basis of that presented expedient Δ_A to introduce as the further characteristic of a number.

Determination. The character of number A we will call value Δ_A, satisfying the condition

$$\Delta_A = \begin{cases} 0, & \text{если } \alpha_n \geqslant S_A^* \text{ и } S_A \geqslant S_A^* \text{ или } \alpha_n < S_A^* \text{ и } S_A < S_A^*, \\ 1, & \text{если } \alpha_n < S_A^* \text{ и } S_A \geqslant S_A^*, \\ -1, & \text{если } \alpha_n \geqslant S_A^* \text{ и } S_A < S_A^*. \end{cases}$$

(3.44)

Key: (1). if. (2). or.

Page 104.

The character of a number is very convenient and compact characteristic. In particular, it proves to be, for the fixation of the fact of overflow during the addition it suffices to know only the character of operands and sum.

§3.6. Criterion of overflow during the addition.

Let be preset two minimum pseudo-orthogonal numbers M_{α_i} and M_{β_i} with digits α_i and β_i on one and the same basis/base p_i with the minimum traces, respectively equal to $S_{\alpha_i}^*$ and $S_{\beta_i}^*$.

We form their sum

$$M = M_{\alpha_i} + M_{\beta_i}$$

or

$$M = (0, 0, \ldots, 0, (\alpha_i + \beta_i)(\bmod p_i), \ldots$$
$$\ldots, (S_{\alpha_i}^* + S_{\beta_i}^*)(\bmod p_n)).$$

The minimum trace of Mach number let us designate through
As is known, minimum trace can take either the value $S^*_{\alpha_i+\beta_i}$.

$$S^*_{\alpha_i+\beta_i} = (S^*_{\alpha_i} + S^*_{\beta_i}) \pmod{p_n},$$
or
$$S^*_{\alpha_i+\beta_i} = (S^*_{\alpha_i} + S^*_{\beta_i} - 1) \pmod{p_n}.$$

Determination. The pair of digits α_i and β_i we will call correct pair, if for the sum of two minimum pseudo-orthogonal numbers M_{α_i} and M_{β_i} occurs the relationship/ratio

$$S^*_{\alpha_i+\beta_i} = (S^*_{\alpha_i} + S^*_{\beta_i}) \pmod{p_n}, \tag{3.45}$$

and the pair of digits α_i, β_i we will call incorrect pair if

$$S^*_{\alpha_i+\beta_i} - (S^*_{\alpha_i} + S^*_{\beta_i} - 1) \pmod{p_n}. \tag{3.46}$$

On the basis of this determination can be formulated the following theorem.

Page 105.

Theorem 3.13 (about the trace of sum). If in the standardized/normalized system are preset two numbers A_1 and A_2:
$$A_1 = (\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_i^{(1)}, \ldots, \alpha_n^{(1)}),$$
$$A_2 = (\alpha_1^{(2)}, \alpha_2^{(2)}, \ldots, \alpha_i^{(2)}, \ldots, \alpha_n^{(2)}),$$
and the sum of these numbers

$$A_1 + A_2 = ((\alpha_1^{(1)} + \alpha_1^{(2)}) \pmod{p_1}, \ (\alpha_2^{(1)} + \alpha_2^{(2)}) \pmod{p_2}, \ldots$$
$$\ldots, (\alpha_n^{(1)} + \alpha_n^{(2)}) \pmod{p_n})$$

and if the sums of the minimum pseudo-orthogonal components of these numbers are M_{A_1}, M_{A_2}, $M_{A_1+A_2}$:

$$M_{A_1} = (\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_{n-1}^{(1)}, S_{A_1}),$$
$$M_{A_2} = (\alpha_1^{(2)}, \alpha_2^{(2)}, \ldots, \alpha_{n-1}^{(2)}, S_{A_2}).$$
$$M_{A_1+A_2} = ((\alpha_1^{(1)} + \alpha_1^{(2)})(\bmod p_1), (\alpha_2^{(1)} + \alpha_2^{(2)})(\bmod p_2), \ldots$$
$$\ldots, (\alpha_{n-1}^{(1)} + \alpha_{n-1}^{(2)})(\bmod p_{n-1}), S_{A_1+A_2}),$$

then the trace of sum occurs the expression

$$S_{A_1+A_2} = (S_{A_1} + S_{A_2} - \delta_{A_1 A_2})(\bmod p_n), \qquad (3.47)$$

where $\delta_{A_1 A_2}$ is a number of incorrect pairs, which are contained in the sequence

$$(\alpha_1^{(1)}, \alpha_1^{(2)}), (\alpha_2^{(1)}, \alpha_2^{(2)}), \ldots, (\alpha_{n-1}^{(1)}, \alpha_{n-1}^{(2)}). \qquad (3.48)$$

Proof. According to the determination

$$S_{A_1} = (S_{\alpha_1^{(1)}}^* + S_{\alpha_2^{(1)}}^* + \ldots + S_{\alpha_{n-1}^{(1)}}^*)(\bmod p_n).$$
$$S_{A_2} = (S_{\alpha_1^{(2)}}^* + S_{\alpha_2^{(2)}}^* + \ldots + S_{\alpha_{n-1}^{(2)}}^*)(\bmod p_n).$$
$$S_{A_1+A_2} = (S_{\alpha_1^{(1)}+\alpha_1^{(2)}}^* + S_{\alpha_2^{(1)}+\alpha_2^{(2)}}^* + \ldots + S_{\alpha_{n-1}^{(1)}+\alpha_{n-1}^{(2)}}^*)(\bmod p_n).$$

Let us compute

$$(S_{A_1} + S_{A_2})(\bmod p_n) = ((S_{\alpha_1^{(1)}}^* + S_{\alpha_1^{(2)}}^*) + \ldots$$
$$\ldots + (S_{\alpha_{n-1}^{(1)}}^* + S_{\alpha_{n-1}^{(2)}}^*))(\bmod p_n).$$

For each value $S_{\alpha_i^{(1)}+\alpha_i^{(2)}}^*$ possibly either (3.45), when $(\alpha_i^{(1)}, \alpha_i^{(2)})$ - correct pair, or (3.46), when $(\alpha_i^{(1)}, \alpha_i^{(2)})$ - incorrect pair. Hence it follows that $S_{A_1+A_2}$ will differ from $S_{A_1} + S_{A_2}$ by a number of incorrect pairs in (3.48), that also comprises the assertion of theorem.

The theorem examined makes it possible to determine trace $S_{A_1+A_2}$ of sum in the values of traces S_{A_1} and S_{A_2} composed without forming of

sum from the minimum pseudo-orthogonal components.

Page 106.

Let us consider now how it is possible to determine the number
of transitions through p_n with formation/education $M_{A_1 + A_2}$ in the
numbers of transitions through p_n with layout M_{A_1} and M_{A_2}.

For this let us introduce the following determination.

Determination. the pair of digits $(\alpha_i^{(1)}, \alpha_i^{(2)})$ we will call standard
pair, if with the addition of two minimum pseudo-orthogonal numbers
occurs inequality

$$S^*_{\alpha_i^{(1)}} + S^*_{\alpha_i^{(2)}} < p_n, \qquad (3.49)$$

and by nonstandard pair, if

$$S^*_{\alpha_i^{(1)}} + S^*_{\alpha_i^{(2)}} \geqslant p_n. \qquad (3.50)$$

Theorem 3.14. If in the standardized/normalized system are
preset numbers A_1, A_2 and their sum $A_1 + A_2$

$$A_1 = (\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_n^{(1)}),$$
$$A_2 = (\alpha_1^{(2)}, \alpha_2^{(2)}, \ldots, \alpha_n^{(2)}),$$
$$A_1 + A_2 = ((\alpha_1^{(1)} + \alpha_1^{(2)}) \, (\mathrm{mod}\, p_1),$$
$$(\alpha_2^{(1)} + \alpha_2^{(2)}) \, (\mathrm{mod}\, p_2), \ldots, (\alpha_n^{(1)} + \alpha_n^{(2)}) \, (\mathrm{mod}\, p_n)),$$

to the correction of ranks of which is respectively equal to $\pi_{A_1}, \pi_{A_2},$
$\pi_{A_1 + A_2}$, then occurs the following equality:

$$\pi_{A_1 + A_2} = \pi_{A_1} + \pi_{A_2} - e_{A_1 A_2} + \xi - \gamma, \qquad (3.51)$$

where ε_{A_1, A_2} are a number of nonstandard pairs in the sequence

$$(\alpha_1^{(1)}, \alpha_1^{(2)}), (\alpha_2^{(1)}, \alpha_2^{(2)}), \ldots, (\alpha_{n-1}^{(1)}, \alpha_{n-1}^{(2)}),$$

but values ε and γ are determined from the conditions:

$$\varepsilon = \begin{cases} 1, & \text{если } S_{A_1} + S_{A_2} \geqslant p_n, \\ 0, & \text{если } S_{A_1} + S_{A_2} < p_n, \end{cases} \qquad (3.52)$$

$$\gamma = \begin{cases} 1, & \text{если } S_{A_1 + A_2} + \delta_{A_1, A_2} \geqslant p_n, \\ 0, & \text{если } S_{A_1 + A_2} + \delta_{A_1, A_2} < p_n. \end{cases} \qquad (3.53)$$

Key: (1). if.

Proof. Regarding the trace of number $A_1 + A_2$ we have

$$S_{A_1 + A_2} = (S^*_{\alpha_1^{(1)} + \alpha_1^{(2)}} + \ldots + S^*_{\alpha_{n-1}^{(1)} + \alpha_{n-1}^{(2)}}) \pmod{p_n}.$$

In the right side of this expression value $S^*_{\alpha_i^{(1)}} + S^*_{\alpha_i^{(2)}}$, where $i = 1, 2,$ ..., $n-1$, will enter either completely, as $S^*_{\alpha_i^{(1)} + \alpha_i^{(2)}}$, if $(\alpha_i^{(1)}, \alpha_i^{(2)})$ - standard pair or as $p_n + S^*_{\alpha_i^{(1)} + \alpha_i^{(2)}}$ otherwise.

Page 107.

Consequently, the right side of this expression will be to value $p_n \varepsilon_{A_1 A_2}$ more than $S_{A_1 + A_2}$, i.e. with formation/education $S_{A_1 + A_2}$ will be perfect on $\varepsilon_{A_1 A_2}$ ⟶ it is less transitions through p_n, than the sum of a number of transitions, obtained with formation/education S_{A_1} and S_{A_2} individually.

Furthermore, with the addition of traces S_{A_1} and S_{A_2} can occur transition on p_n, if $S_{A_1} + S_{A_2} \geqslant p_n$, which was not considered during

calculation $S_{A_1+A_2}$. consequently, the sum of the corrections of ranks must be additionally increased to a number ξ.

On the sum of traces S_{A_1} and S_{A_2} it can be represented in the form

$$S_{A_1} + S_{A_2} = \xi p_n + s. \qquad (3.54)$$

where s - whole non-negative number.

Taking into account that $s < p_n$, we on the basis (3.47) and (3.54) will obtain

$$S_{A_1+A_2} = (s - \delta_{A_1 A_2}) \,(\mathrm{mod}\, p_n).$$

When occurs the relationship/ratio

$$s > \delta_{A_1 A_2},$$

the refinement of the sum of the corrections of ranks is not required. In this case

$$S_{A_1+A_2} = s - \delta_{A_1 A_2}$$

or

$$S_{A_1+A_2} + \delta_{A_1 A_2} = s < p_n,$$

i.e. equality (3.51) occurs.

In the case when

$$s < \delta_{A_1 A_2},$$

the trace of sum is defined as

whence $$S_{A_1+A_2} = p_n + s - \delta_{A_1 A_2},$$

$$S_{A_1+A_2} + \delta_{A_1 A_2} = p_n + s > p_n.$$

and the sum of the corrections of ranks must be reduced per unit, that also is reflected in equality (3.51), which composes the assertion of theorem.

Page 108.

Theorem 3.15. If in the standardized/normalized system are preset numbers A_1, A_2 and their sum $A_1 + A_2$:

$$A_1 = (\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_n^{(1)}),$$
$$A_2 = (\alpha_1^{(2)}, \alpha_2^{(2)}, \ldots, \alpha_n^{(2)}),$$
$$A_1 + A_2 = ((\alpha_1^{(1)} + \alpha_1^{(2)}) \,(\mathrm{mod}\, p_1), \ldots, (\alpha_n^{(1)} + \alpha_n^{(2)}) \,(\mathrm{mod}\, p_n))$$

with ranks $r_{A_1}, r_{A_2}, r_{A_1+A_2}$ and kernels $K_{A_1}, K_{A_2}, K_{A_1+A_2}$ of these ranks, respectively then the kernel of the rank of the sum $A_1 + A_2$ is determined by the expression

$$K_{A_1+A_2} = K_{A_1} + K_{A_2} - m_{A_1+A_2} - e_{A_1A_2}, \qquad (3.55)$$

where

$$m_{A_1+A_2} = \sum_{i=1}^{n-1} \eta_i m_i \qquad (3.56)$$

and

$$\eta_i = \begin{cases} 1, & \text{если } \alpha_i^{(1)} + \alpha_i^{(2)} \geqslant p_i, \\ 0, & \text{если } \alpha_i^{(1)} + \alpha_i^{(2)} < p_i, \end{cases} \qquad (3.57)$$
$$i = 1, 2, \ldots, n.$$

Key: (1). if.

Proof. Let us consider minimum pseudo-orthogonal numbers $M_{\alpha_i^{(1)}}$ and $M_{\alpha_i^{(2)}}$ on basis/base p_i with ranks $r_{\alpha_i^{(1)}}$ and $r_{\alpha_i^{(2)}}$ respectively.

Since with the addition of two minimum pseudo-orthogonal numbers

it cannot be derating $[0, \mathscr{P})$, then true rank $\bar{r}_{\alpha_i^{(1)}+\alpha_i^{(2)}}$ of the sum of these numbers coincides with the calculated rank of sum $r_{\alpha_i^{(1)}+\alpha_i^{(2)}}$ which is defined as

i.e.

$$\bar{r}_{\alpha_i^{(1)}+\alpha_i^{(2)}} = r_{\alpha_i^{(1)}} + r_{\alpha_i^{(2)}} - \eta_i m_i - \eta_n,$$

$$r_{\alpha_i^{(1)}+\alpha_i^{(2)}} = \bar{r}_{\alpha_i^{(1)}+\alpha_i^{(2)}} = r_{\alpha_i^{(1)}} + r_{\alpha_i^{(2)}} - \eta_i m_i - \eta_n.$$

Summarizing both parts of this equality on i from i=1 to i=n-1, we will obtain

$$K_{A_1+A_2} = K_{A_1} + K_{A_2} - m_{A_1+A_2} - \varepsilon_{A_1, A_2},$$

that also composes the assertion of theorem.

Theorem 3.16. If in the standardized/normalized system are preset numbers A_1 and A_2 and their sum A_1+A_2 with ranks r_{A_1}, r_{A_2}, $r_{A_1+A_2}$, by the kernels of ranks K_{A_1}, K_{A_2}, $K_{A_1+A_2}$, by the corrections of ranks π_{A_1}, π_{A_2}, $\pi_{A_1+A_2}$ and characteristics Δ_{A_1}, Δ_{A_2}, $\Delta_{A_1+A_2}$ respectively, then true rank $r_{A_1+A_2}$ of sum A_1+A_2 is equal to

$$r_{A_1+A_2} = K_{A_1} + K_{A_2} - m_{A_1+A_2} - \pi_{A_1} - \pi_{A_2} - \Delta_{A_1+A_2} - \xi + \gamma.$$

$$(3.58)$$

Page 109.

Proof. Since the true rank of sum is determined by the expression

$$r_{A_1+A_2} = K_{A_1+A_2} - \pi_{A_1+A_2} - \Delta_{A_1+A_2},$$

then, after placing in the right side of this equality value $K_{A_1+A_2}$ from (3.55) and value $\pi_{A_1+A_2}$ from (3.51), we will obtain

$$r_{A_1+A_2} = K_{A_1} + K_{A_2} - m_{A_1+A_2} - \varepsilon_{A_1, A_2} - \pi_{A_1} -$$
$$- \pi_{A_2} + \varepsilon_{A_1, A_2} - \xi + \gamma - \Delta_{A_1+A_2}.$$

This expression after decrease ε_{A_1, A_2} passes in (3.58).

Let us formulate now the theorem about the criterion of overflow with addition of two numbers.

Theorem 3.17. (About the criterion of overflow during addition). If in the standardized/normalized system are preset two positive numbers: A_1, A_2, their sum $A_1 + A_2$ with characters Δ_{A_1}, Δ_{A_2}, $\Delta_{A_1 + A_2}$ respectively, then the single value of value Ω

$$\Omega = \Delta_{A_1} + \Delta_{A_2} + \eta_n - \Delta_{A_1 + A_2} - \xi + \gamma \qquad (3.59)$$

indicates that with the addition occurred the overflow, and zero value Ω testifies about the absence of overflow.

Proof. In accordance with the theorem about calculated rank $\bar{r}_{A_1 + A_2}$ of sum we can write

$$\bar{r}_{A_1 + A_2} = r_{A_1} + r_{A_2} - \sum_{i=1}^{n-1} \eta_i m_i - \eta_n = r_{A_1} + r_{A_2} - m_{A_1 + A_2} - \eta_n.$$

After expressing values r_{A_1} and r_{A_2} through the kernels of ranks, the correction of ranks and characters, we will obtain

$$\bar{r}_{A_1 + A_2} = K_{A_1} - \pi_{A_1} - \Delta_{A_1} + K_{A_2} - \pi_{A_2} - \Delta_{A_2} - m_{A_1 + A_2} - \eta_n.$$
$$(3.60)$$

Let us designate through Ω the difference between the true and calculated rank of the sum

$$\Omega = r_{A_1 + A_2} - \bar{r}_{A_1 + A_2}.$$

Page 110.

After substituting here value $r_{A_1+A_2}$ from (3.58) and value $\bar{r}_{A_1+A_2}$ from (3.60), we will obtain

$$\Omega = \Delta_{A_1} + \Delta_{A_2} + \eta_n - \Delta_{A_1+A_2} - \xi + \gamma.$$

It is known that in the absence of overflow the true rank coincides with the calculated, i.e., $\Omega=0$, and in the presence of overflow calculated rank is less than the real rank by one, i.e., $\Omega=1$, that also composes the assertion of theorem.

The examined criterion of overflow during the addition of two numbers can be generalized to an arbitrary number of components/terms/addends.

Generalized theorem 3.18 (about the criterion of overflow during the addition). If in the standardized/normalized system are preset positive numbers A_1, A_2, ..., A_m their their sum

$$A = A_1 + A_2 + \ldots + A_m$$

with the characters respectively Δ_{A_1}, Δ_{A_2}, ..., Δ_{A_m}, Δ_A, the zero value of value

$$\Omega_A = \sum_{i=1}^{m} \Delta_{A_i} + \sum_{i=2}^{m} \eta_{n,i} - \Delta_A - \sum_{i=2}^{m} \xi_i + \sum_{i=2}^{m} \gamma_i, \quad (3.61)$$

where

$$\eta_{n,\,i+1} = \begin{cases} 1, \text{ если при сложении суммы} \\ A^{(i)} = \sum_{j=1}^{i} A_j \text{ с числом } A_{i+1} \text{ имел} \\ \text{место переход по основанию } p_n, \\ 0 - \text{в остальных случаях;} \end{cases} \quad (3.62)$$

$$\xi_{i+1} = \begin{cases} 1, \text{ если } S_{A^{(i)}} + S_{A_{i+1}} \geqslant p_n, \\ 0, \text{ если } S_{A^{(i)}} + S_{A_{i+1}} < p_n; \end{cases} \quad (3.63)$$

$$\gamma_{i+1} = \begin{cases} 1, \text{ если } S_{A^{(i+1)}} + \delta_{i+1} \geqslant p_n, \\ 0, \text{ если } S_{A^{(i+1)}} + \delta_{i+1} < p_n; \end{cases} \quad (3.64)$$

Key: (1). if during the addition of sum. (2). with number A_{i+1} occurred

transition on basis/base p_n, 0 - in remaining cases. (3). if.

$(\delta_i -$ a number of incorrect pairs in numbers $A^{(i)}$ and $A_{i+1})$ testifies

about the absence of overflow, and the nonzero value of value Ω_A

indicates the fact that with the addition it occurred overflow.

Proof. Nonappearance from range $[0, \mathcal{P})$ of sum from m of

components/terms/addends assumes that had point of emergence from the

range not on one of the intermediate stages of addition, i.e.,

$$\left. \begin{aligned} \Omega_{A^{(2)}} &= 0, \\ \Omega_{A^{(3)}} &= 0, \\ \dots \dots \dots \\ \Omega_{A^{(m)}} &= 0. \end{aligned} \right\} \quad (3.65)$$

Page 111.

From the first expression of condition (3.65) we will obtain

$$\Omega_{A^{(2)}} = \Delta_{A_1} + \Delta_{A_2} + \eta_{n,2} - \Delta_{A_1 + A_2} - \xi_2 + \gamma_2 = 0,$$

whence

$$\Delta_{A_1 + A_2} = \Delta_{A_1} + \Delta_{A_2} + \eta_{n,2} - \xi_2 + \gamma_2.$$

Let us assume now that is satisfied the condition

$$\Omega_{A^{(i)}} = 0$$

and for it it is correct

$$\Delta_{A^{(i)}} = \sum_{j=1}^{i} \Delta_{A_j} + \sum_{j=2}^{i} \eta_{n,j} - \sum_{j=2}^{i} \xi_j + \sum_{j=2}^{i} \gamma_j. \qquad (3.66)$$

Let us compute now value $\Omega_{A^{(i+1)}}$:

$$\Omega_{A^{(i+1)}} = \Delta_{A^{(i)}} + \Delta_{A_{i+1}} + \eta_{n,i+1} - \Delta_{A^{(i+1)}} - \xi_{i+1} + \gamma_{i+1}.$$

After substituting here value $\Delta_{A^{(i)}}$ from (3.66), we will obtain

$$\Omega_{A^{(i+1)}} = \sum_{j=1}^{i+1} \Delta_{A_j} + \sum_{j=2}^{i+1} \eta_{n,j+1} - \Delta_{A^{(i+1)}} - \sum_{j=2}^{i+1} \xi_j + \sum_{j=2}^{i+1} \gamma_j.$$

Thus showed that if expression (3.61) occurs with the addition i of the numbers

$$A^{(i)} = \sum_{j=1}^{i} A_j,$$

then it is correct with addition i+1 of the numbers

$$A^{(i+1)} = \sum_{j=1}^{i+1} A_j.$$

Applying the method of induction, we prove validity (3.61) for any i, in the final analysis for i=π, that also composes the assertion of the generalized theorem.

Page 112.

§3.7. Representation of numbers. Introduction of the sign of a

number. Rule of signs.

The system of residual classes is very efficient with the fulfillment of rational operations, noticeably it is complicated with the fulfillment of such operations in the arithmetic unit, during which is required the knowledge of entire number, i.e., its positional value.

The introduced concept of the rank of a number, which makes it possible to in principle solve the problems, which relate to the evaluation of entire number as a whole, nevertheless possesses the deficiency/lack, connected, on one hand, with the fact that the value of the rank of a number is not modular, but on the other hand, by the position of the determination of the rank of a number into the positional system of counting.

By introduction of rank we introduce to the representation of a number element/cell of position. Very representation of a number becomes heterogeneous and, naturally, in this case hinder the nonpositional operations on a number. By the possible method of overcoming this difficulty is the replacement of rank the character of a number. In certain cases is considered by advisable the enlistment of the trace of a number - modular value.

Both the character and trace numbers, being modular values, at
the same time carry information about its positional representation,
in other words about the location of a number relative to the first
interval of numerical range.

To us seems by sufficiently successful very fact of the
enlistment of modular values, which do not break the uniformity of
the representation of a number, but which at the same time carry
information about its positional value.

Thus, speaking about a number in the system of residual classes,
we will consider that to us are known its remainders/residues on
bases/bases $p_1, p_2, \ldots, p_n$, trace S_A on basis/base p_n and character
Δ_A.

Theorem 3.19. If in the standardized/normalized system are
preset the minimum pseudo-orthogonal numbers

$$M_{\alpha_i} = (0, 0, \ldots, 0, \alpha_i, 0, \ldots, S_{\alpha_i}^*),$$
$$M_{p_i - \alpha_i} = (0, 0, \ldots, 0, p_i - \alpha_i, 0, \ldots, S_{p_i - \alpha_i}^*)$$

and if $\alpha_i \neq 0$, then pair $(\alpha_i, p_i - \alpha_i)$ is incorrect.

Proof. As is known, under the conditions of the theorem

$$S_{\alpha_i}^* + S_{p_i - \alpha_i}^* = p_n + 1,$$

and the minimum trace of the sum of numbers M_{α_i} and $M_{p_i - \alpha_i}$ is defined as

Page 113.

$$S^*_{\alpha_i+(p_i-\alpha_i)} = S^*_{p_i} \equiv 0 \,(\mathrm{mod}\,p_n).$$

Hence

$$S^*_{\alpha_i+(p_i-\alpha_i)} = (S^*_{\alpha_i} + S^*_{p_i-\alpha_i} - 1)\,(\mathrm{mod}\,p_n),$$

that in accordance with the determination confirms inaccuracy of pair $(\alpha_i,\ p_i-\alpha_i)$.

Theorem 3.20. (About the sum of traces). In the standardized/normalized system trace S_A of number A, which has μ_A different from zero ones digits in bases/bases p_1, p_2, ..., p_{n-1}, and trace $S_{\mathscr{P}-A}$ further to A number $\mathscr{P}-A$ are connected with the relationship/ratio

$$(S_A + S_{\mathscr{P}-A})\,(\mathrm{mod}\,p_n) = \mu_A. \qquad (3.67)$$

Proof. As can easily be seen, the trace of the sum of a number with its addition to $\mathscr{P}$ exists

$$S_{A+(\mathscr{P}-A)} = S_{\mathscr{P}} \equiv 0\,(\mathrm{mod}\,p_n).$$

On the other hand, the sum of the traces of a number and its addition to $\mathscr{P}$ satisfies the relationship/ratio

$$S_A + S_{\mathscr{P}-A} - \delta_{A,\mathscr{P}-A} = S_{A+(\mathscr{P}-A)}\,(\mathrm{mod}\,p_n),$$

where $\delta_{A,\mathscr{P}-A}$ — number of incorrect pairs among $(\alpha_i, p_i-\alpha_i)$, i=1, 2, ..., n-1.

According to the previous theorem a number of incorrect pairs coincides with μ_A— i.e. with a number of nonzero digits in a number A. Hence

$$(S_A + S_{\mathscr{P}-A})(\bmod\, p_n) = \mu_A,$$

that also composes the assertion of theorem.

Corollary. if number A with trace S_A and number of nonzero digits μ_A, then the trace of a further number is preset is determined by the relationship/ratio

$$S_{\mathscr{P}-A} = \begin{cases} \mu_A - S_A, & \overset{(1)}{\text{если}}\ \mu_A \geqslant S_A, \\ p_n + \mu_A - S_A, & \text{если}\ \mu_A < S_A. \end{cases} \quad (3.68)$$

Key: (1). if.

Page 114.

Theorem 3.21. (About the character of a further number). In the numbered system character Δ_A of number A is connected with character $\Delta_{\mathscr{P}-A}$ of further number $\mathscr{P}-A$ with the relationship/ratio

$$\Delta_{\mathscr{P}-A} = \begin{cases} -\Delta_A, & \overset{(1)}{\text{если}}\ \alpha_n \neq 0\ \overset{(2)}{\text{и}}\ \mu_A \geqslant S_A, \\ 1, & \text{если}\ \alpha_n = 0\ \text{и}\ \mu_A < S_A, \\ 1 - \Delta_A, & \text{если}\ \alpha_n = 0\ \text{и}\ \mu_A \geqslant S_A \\ & \overset{(3)}{\text{или}}\ \alpha_n \neq 0\ \text{и}\ \mu_A < S_A, \end{cases} \quad (3.69)$$

Key: (1). if. (2). and. (3). or.

where μ_A— number of nonzero digits of number A on bases/bases p_1,

$p_2, \ldots, p_{n-1}$.

Proof. Let us consider the sum of number A with its addition to $\mathscr{P}$

$$A + (\mathscr{P} - A) = \mathscr{P}.$$

With the addition occurs the overflow, i.e., $\Omega = 1$, furthermore, character and the trace of sum equal to zero

$$\Delta_{A + (\mathscr{P} - A)} = 0; \quad S_{A + (\mathscr{P} - A)} = 0,$$

whence

$$S_{A + (\mathscr{P} - A)} + \delta_{A, \mathscr{P} - A} = \delta_{A, \mathscr{P} - A} < p_n \text{ и } \gamma = 0. \qquad (1)$$

Key: (1). and.

The criterion of overflow during the addition accepts the form

$$\Omega = \Delta_A + \Delta_{\mathscr{P} - A} + \eta_n - \xi$$

or

$$\Delta_{\mathscr{P} - A} = 1 - \Delta_A - \eta_n + \xi. \qquad (3.70)$$

We analyze the possible cases when $\alpha_n = 0$. Transition through p_n with addition α_n and $p_n - \alpha_n$ will not occur and, therefore, $\eta_n = 0$, i.e. (3.70) it passes in

$$\Delta_{\mathscr{P} - A} = 1 - \Delta_A + \xi.$$

Are here possible two cases.

Case 1. If $\mu_A > S_A$, then $S_{\mathscr{P} - A} = \mu_A - S_A$ and with addition $S_A + S_{\mathscr{P} - A}$ there will not be transition through p_n. Consequently, $\xi = 0$ and $\Delta_{\mathscr{P} - A} = 1 - \Delta_A$,

which corresponds (3.69).

Case   2. If $\mu_A < S_A$, then $S_{\mathscr{P}-A} = \mu_A + p_n - S_A$, in sum $S_A + S_{\mathscr{P}-A}$ will occur transition through p_n, i.e. $\varepsilon = 1$ and

$$\Delta_{\mathscr{P}-A} = 2 - \Delta_A. \qquad (3.71)$$

Page 115.

However, since Δ_A and $\Delta_{\mathscr{P}-A}$ can take only values of 0.1 and -1, the equality (3.71) is possible only with

$$\Delta_{\mathscr{P}-A} = \Delta_A = 1,$$

which coincides with (3.69). Then that in this case $\Delta_A = 1$, it is completely understandable. Here S_A is greater than quantity μ_A of nonzero digits in A, and it is possible to claim that occurs the situation

$$\alpha_n = 0 < S_A^* \leqslant S_A,$$

which determines $\Delta_A = 1$.

Now let $\alpha_n \neq 0$.

Then there must take   place transition through p_n with addition $\alpha_n + p_n - \alpha_n$, i.e. $\eta_n = 1$ and (3.70) passes in

$$\Delta \mathscr{P}_{-A} = \xi - \Delta_A. \qquad (3.72)$$

Here are also possible two cases.

Case 1. If $\mu_A \geqslant S_A$, then $\xi = 0$ and $\Delta \mathscr{P}_{-A} = -\Delta_A$, which coincides with (3.69).

Case 2. If $\mu_A < S_A$, then $\xi = 1$ and (3.72) passes into the expression

$$\Delta \mathscr{P}_{-A} = 1 - \Delta_A,$$

which also coincides with (3.69).

Thus, the theorems examined allow for us on the trace and character of an initial number to unambiguously determine trace and character of a further number. Let us now move on to the study of the problem about the introductions the signs of a number.

Earlier was examined the version of the introduction of the artificial form of numbers to which both negative and positive numbers they were represented as positive numbers, moreover were established/installed such rules of the execution of the operations which ensured the correctness of result both in the value and on the sign. In this version the positive numbers are represented by numbers

in interval $[\bar{P}, \mathscr{P})$, and negative $[0, \bar{P})$.

If we among the basis of system eat the basis/base, equal to
two, for example $p_1 = 2$, then it is possible to consider that the
numbers, which lie in the range $[0, \mathscr{P}/2)$, are negative, and in the range
$[\mathscr{P}/2, \mathscr{P})$ — positive. Number itself $\mathscr{P}/2$ can be accepted as computer zero.
Thus, a question of the determination of the sign of a number is
equivalent to the determination of the interval in which this number
is located.

Page 116.

For the case when one of the bases/bases is equal to two ($p_1 = 2$)
it is possible to claim that the number
$$A_0 = (0, \alpha_2, \ldots, \alpha_n) \quad \text{и} \quad A_1 = (1, \alpha_2, \ldots, \alpha_n)$$
Key: (1). and.

have different signs, since they lie/rest at the different intervals
relative to $\mathscr{P}/2$.

Let us formulate the theorem, which makes it possible in a
number of cases to immediately determine sign of a number.

Theorem 3.22. (About the sign of a number). If in the

standardized/normalized system with bases/bases $p_1=2$, p_2, $...$, p_n are preset numbers A of form $A(\alpha_1, \alpha_2, ..., \alpha_n)$ with minimum traces S_A^*, then all numbers, for which is fulfilled the inequality

$$\alpha_n - S_A^* + 1 \leqslant \frac{p_n - 1}{2},\qquad(3.73)$$

they are negative, and all numbers, for which is fulfilled the inequality

$$\alpha_n - S_A^* \geqslant \frac{p_n + 1}{2},\qquad(3.74)$$

they are positive.   Proof. Number A enclosed in the limits

$$(\alpha_n - S_A^*)\frac{\mathscr{P}}{p_n} \leqslant A < (\alpha_n - S_A^* + 1)\frac{\mathscr{P}}{p_n}.$$

Consequently, if

$$(\alpha_n - S_A^* + 1)\frac{\mathscr{P}}{p_n} < \frac{\mathscr{P}}{2},\qquad(3.75)$$

then $A < \mathscr{P}/2$ is negative. However, since

$$\frac{\mathscr{P}}{2} = \frac{\mathscr{P}}{p_n}\frac{p_n}{2},$$

that (3.75) it is possible to rewrite in the form

$$\alpha_n - S_A^* + 1 < \frac{p_n}{2}.$$

Taking into account that basis/base p_n — odd, we, passing from $p_n/2$ to $(p_n-1)/2$, we can write negativity condition of number A in the form (3.73).

Analogously from the condition

$$(\alpha_n - S_A^*)\frac{\mathscr{P}}{p_n} > \frac{\mathscr{P}}{2}$$

we will obtain the condition of the positiveness of number A (3.74), after replacing $p_n/2$ by $(p_n + 1)/2$.

Page 117.

The theorem examined about the sign of a number with the known

minimum trace of number S_A^* allows on inequalities (3.73) and (3.74)

to determine the sign of a number, leaving not defined only the case

when number A is such, that

$$\alpha_n - S_A^* < \frac{p_n + 1}{2},$$
$$\alpha_n - S_A^* + 1 > \frac{p_n - 1}{2}.$$

In other words not defined is the case of a small in the absolute

value number A, when A is included

$$\left[\frac{p_n - 1}{2} \frac{\mathcal{P}}{p_n}, \; \frac{p_n + 1}{2} \frac{\mathcal{P}}{p_n} \right),$$

i.e. it is located in the interval of length $\mathcal{P}/p_n$, containing point

$\mathcal{P}/2$ as the center of symmetry. It is obvious, at this interval they

lie/rest both positive and negative numbers and therefore one fact

alone of determination A in this interval it is still insufficient

for determining the sign A.

For explaining the sign A in this indefinite case, it is

possible to enter as follows. Let us consider the number

$$A' = A + \frac{\mathcal{P}}{2} = A + (1, 0, \ldots, 0).$$

According to the determination of the sign of number sign A'

=-sign A. At the same time number A' does not lie/rest at the

interval of uncertainty/indeterminancy and if is known minimum trace

S_A^*, then sign A' will be determined in accordance with inequalities (3.73), (3.74), but on sign A' will be determined sign A. Thus, with known minimum traces S_A^* and $S_{A'}^*$ a question about the sign of a number is solved by the simple analysis of difference $\alpha_n - S_A^*$ and $\alpha_n - S_{A'}^*$. Let us formulate the analogous theorem about the determination of the sign of a number through S_A, taking into account that

$$\alpha_n - S_A \leqslant \alpha_n - S_A^*,$$
$$\alpha_n - S_A \geqslant \alpha_n - S_A^* - n + 2 - \omega.$$

Theorem 3.23. If in the standardized/normalized system with bases/bases $p_1 = 2$, p_2, ..., p_n are preset numbers A of form $A = (x_1, x_2, ..., \alpha_n)$ with trace S_A, then all numbers, for which occurs the inequality

$$\alpha_n - S_A + 1 \leqslant \frac{p_n - 1}{2} - (n - 2 - \omega). \qquad (3.76)$$

they are negative, and all numbers, for which occurs the inequality

$$\alpha_n - S_A \geqslant \frac{p_n + 1}{2}, \qquad (3.77)$$

they are positive.

Page 118.

Here also we have a region of uncertainty/indeterminancy which already considerably wider is characterized by the inequalities

$$\alpha_n - S_A < \frac{p_n + 1}{2},$$
$$\alpha_n - S_A + 1 > \frac{p_n - 1}{2} - (n - 2 - \omega).$$

In other words and here the region of uncertainty/indeterminancy is located near $\mathcal{P}/2$, on both sides from it, but in view of the dissymmetry of evaluation S_A^* through S_A this region is unsymmetrical relatively $\mathcal{P}/2$. Furthermore, during use S_A^* for the definition of the interval of determination A we take $\alpha_n - S_A^*$ when $\alpha_n \geqslant S_A^*$ and $p_n + \alpha_n - S_A^*$ when $\alpha_n < S_A^*$, while during use S_A, it cannot be in all cases when $\alpha_n < S_A$ taken $p_n + \alpha_n - S_A$ without the analysis of the character of number Δ_A.

Let us consider the method of determining the sign of a number based on specific example.

Let be preset the system of the bases/bases

$$p_1 = 2, \quad p_2 = 5, \quad p_3 = 7, \quad p_4 = 23.$$

Let us give minimum pseudo-orthogonal numbers for the selected system of the bases/bases

$$M_{11} = (1, 0, 0, 12) \quad M_{24} = (0, 4, 0, 14) \quad M_{34} = (0, 0, 4, 14)$$
$$M_{21} = (0, 1, 0, 10) \quad M_{31} = (0, 0, 1, 4) \quad M_{35} = (0, 0, 5, 17)$$
$$M_{22} = (0, 2, 0, 19) \quad M_{32} = (0, 0, 2, 7) \quad M_{36} = (0, 0, 6, 20)$$
$$M_{23} = (0, 3, 0, 5) \quad M_{33} = (0, 0, 3, 10)$$

Example. To determine the sign of number $(1, 1, 6, 22)$.

Let us compute the trace of number A

$$S_A = (12 + 10 + 20) \,(\text{mod } 23) = 19.$$

Let us compute

$$a_n - S_A = 22 - 19 = 3;$$
$$\frac{p_n - 1}{2} = 11;$$
$$n - 2 - \omega = 2;$$
$$\frac{p_n - 1}{2} - (n - 2 - \omega) = 11 - 2 = 9.$$

Here is satisfied the condition (3.76), i.e., $3 - 1 < 9$; whence number A is negative.

.

Page 119.

When is known the character of number Δ_A, then the sign of a number can be determined on the basis of the criterion of overflow. Let be known trace S_A and character Δ_A of number A. We form the sum

$$A' = A + \frac{\mathscr{P}}{2} = A + (1, 0, 0, \ldots, 0)$$

and let us compute the criterion of overflow Ω. It is obvious, if $\Omega = 1$, overflow occurred and $A > \frac{\mathscr{P}}{2}$, which determines the positive sign of number A. When $\Omega = 0$, we obtain $A < \frac{\mathscr{P}}{2}$, i.e. A negative.

Let us consider expression for Ω. Number $\frac{\mathscr{P}}{2}$, as is known, has trace $S_{\frac{\mathscr{P}}{2}} = \frac{p_n + 1}{2}$ and character $\Delta_{\frac{\mathscr{P}}{2}} = 1$. Then

$$\Omega = \Delta_A + 1 - \Delta_{A + \frac{\mathscr{P}}{2}} - \xi + \gamma.$$

Value η_n is here equal to zero and therefore it is omitted in the expression for Ω.

The method of using the criterion of overflow for determining
the sign of a number is very simple; however, he assumes the
knowledge of characters Δ_A and $\Delta_{A+\frac{\mathscr{P}}{2}}$, in connection with which is
interesting to note the close interconnection between the sign of a
number and its character - knowledge of one of these values it
contributes to the determination of another.

In the case when character Δ_A it is directly difficult to
define, and is possible to define Δ_{2A}, where 2A it is understood as the
result of addition A+A, to the target leads the following method. Let
us suppose number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ negative.

1. Is computed $2A = (0, \beta_2, \beta_3, \ldots, \beta_n)$, S_{2A},   and Δ_{2A}.

2. Is determined digit ρ of quotient 2A/2 on basis/base β_1 on
the basis of the fact that digit ρ according to our condition is
always digit of negative number.

3. Is checked agreement of digits α_1 and ρ.

If $\alpha_1 = \rho$, then correctly our assumption about the fact that A -
negative number.

But if $\alpha_1 = 1-\rho$, A - positive number.

1.0

1.1

1.25 1.4 1.6

4.5
5

2.8 2.5
3.2 2.2
3.6
4.0 2.0

1.8

MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU
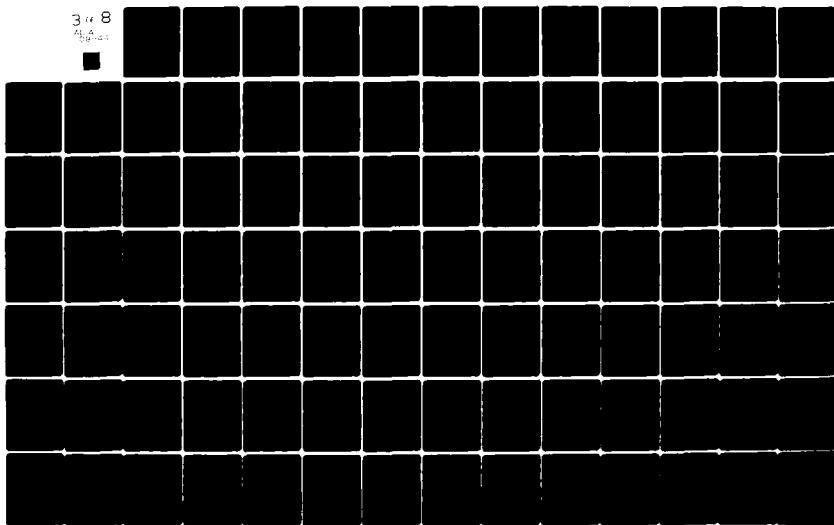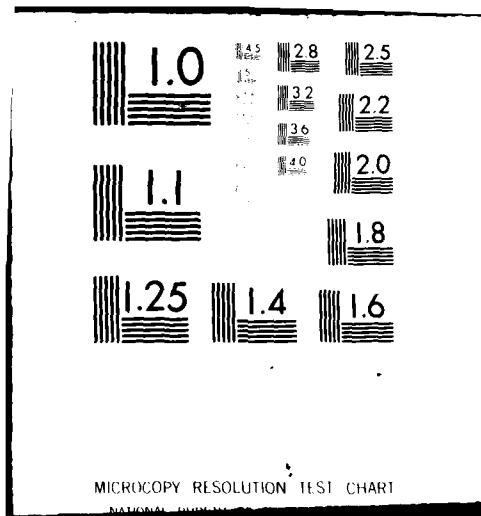
Page 120.

Let us examine an example in the system with bases/bases $p_1=2$, $p_2=5$, $p_3=7$, $p_4=23$.

Example. To determine the sign of number $A=(1, 1, 1, 2)$ by the method cf doubling.

We compute $2A=(0, 2, 2, 4)$; $S_{2A}=(19+7)(\mathrm{mod}\,23)=3$. We compute $\frac{(0, 2, 2, 4)}{(0, 2, 2, 2)}=(1, 1, 1, 2)$. Here $\alpha_1=\rho_1=1$, i.e., an initial number negative $A<0$.

Let us examine now how can be introduced in an explicit form the sign of a number.

We will accompany each number A by its sign sing A. Let us agree that the digit of this bit is equal to zero, if $A \geqslant 0$, and to unity, if $A<0$.

Let us examine different cases of the establishment of the sign of result with the operation/process of addition.

Case 1. $A_1 = +|A_1|, \quad A_2 = +|A_2|$

Sum $A_1 + A_2$ is here positive and it should be ascribed plus sign.
It is necessary by the use/application of a criterion of overflow to
establish fact of output/yield or nonappearance of result from range
$(0, \mathscr{P})$.

Case of 2. $A_1 = -|A_1|, \quad A_2 = -|A_2|$

This case is symmetrical previous. Sum is calculated normally,
by it is assigned minus sign. It is necessary to explain by means of
the criterion of overflow, did take place from range $(0, \mathscr{P})$.

Case of 3. $A_1 = +|A_1|, \quad A_2 = -|A_2|$

Is calculated the sum

$$S = |A_1| + (\mathscr{P} - |A_2|).$$

Here overflows be cannot and the criterion of overflow must be
used for the purpose of the determination of sign. Actually/really,
if $|A_1| > |A_2|$, then difference $|A_1| - |A_2|$ is positive and the sign of result is
positive. But then

$$S = \mathscr{P} + (|A_1| - |A_2|)$$

will contain excess $\mathscr{P}$, here must occur overflow. Thus, here plus sign must accompany sum of S, if $\Omega = 1$, where

$$\Omega = \Delta_{|A_1|} + \Delta_{\mathscr{P} - |A_2|} + \eta_n - \Delta_{|A_1| + \mathscr{P} - |A_2|} - \xi + \gamma,$$

moreover η_n indicates transition on basis/base p_n during the addition of the digits

$$\alpha_n^{(1)} + (p_n - \alpha_{n_j}^{(1)}),$$

where $\alpha_n^{(1)}$ and $\alpha_n^{(2)}$ - digit of numbers $\left|A_1\right|$ and $\left|A_2\right|$ respectively on basis/base p_n.

Page 121.

Value ξ reflects transition on basis p_n during the addition of the traces

$$S_{|A_1|} + S_{\mathscr{P} - |A_2|}.$$

Let us examine now the situation when $|A_1| < |A_2|$.

Here difference $\left|A_1\right| - \left|A_2\right|$ is negative and the sign of result is negative. Then the sum

$$S = \mathscr{P} + (|A_1| - |A_2|) = \mathscr{P} - (|A_2| - |A_1|) < \mathscr{P}$$

will not contain excess $\mathscr{P}$, overflow will not occur and $\Omega = 0$. In this case the result will be represented in the form of object to $\mathscr{P}$ and for the subsequent use must be undertaken a supplemental to it number.

Case of 4. $A_1 = -|A_1|, \quad A_1 = +|A_2|$

Is calculated sum $S = \mathscr{P} - |A_1| + |A_2|$. This case is symmetrical previous with the change by the roles of components/terms/addends.

Thus, for the operation/process of addition with numbers of different signs, the sign of result can be determined according to the criterion of overflow.

In this case there can be formulated following rule of the determination of the sign of sum.

Rule of signs during the addition. During the addition of numbers with the different signs, negative component/term/addend is replaced by its object to $\mathscr{P}$.

In this case the sign of the obtained sum is positive and result is obtained in the natural form, if occurred overflow $\Omega = 1$.

If overflow did not take place ($\Omega = 0$), then the sign of sum was negative and result was obtained in the form of object to $\mathscr{P}$.

§3.8. Formal division.

Let us examine the simplest case when dividend completely is divided into the divider/denominator.

Let be given two numbers in the system with bases/bases $p_1, p_2, \ldots, p_n$, namely: $\bar{A} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $B = (\beta_1, \beta_2, \ldots, \beta_n)$ and let number $C = (\gamma_1, \gamma_2, \ldots, \gamma_n)$ be quotient of the division of A into B, i.e.

$$C = \frac{A}{B}$$

or

$$A = BC.$$

For product BC we will obtain the expression

$$BC = (\gamma_1\beta_1 - k_1 p_1, \ldots, \gamma_n\beta_n - k_n p_n),$$

where k_i - whole non-negative number, which satisfies the condition

$$k_i < p_i, \quad i = 1, 2, \ldots, n.$$

Equalizing BC to A, we will obtain

$$\gamma_i = \frac{\alpha_i + k_i p_i}{\beta_i}. \qquad (3.78)$$

Expression (3.78) uniquely determines the digits of quotient. Thus, division in the case when it is accurately feasible (i.e. when A multiply B), can be realized by a step-by-step division of digits α_i on β_i, here step-by-step division is understood in the sense that if α_i is not directly divided completely into β_i, then to α_i it is added so many once p_i, so that $\alpha_i + k_i p_i$ would be divided completely into β_i $(i = 1, 2, \ldots, n)$.

Under condition $k_i < p_i$ this division in a single manner will determine digit γ_i. Let us note that this division is possible under supplemental condition $\beta_i \neq 0$.

Very important role plays division into 2 and generally on degree 2^k.

Essential is here the absence or the presence among the bases/bases even numbers, and in particular number 2. We begin examination from the case when among the bases/bases even numbers it is not contained.

Let A — even dividend, for which are known S_A, Δ_A. Let it be further

$$\frac{A}{2} = (\beta_1, \beta_2, \ldots, \beta_n).$$

Let us designate through $S_{\frac{A}{2}}$ and $\Delta_{\frac{A}{2}}$ respectively trace and character of number $A/2$.

Determination. Let us name/call digit α_i of correct, if $(\alpha_i/2, \alpha_i/2)$ is correct pair, and incorrect otherwise.

Let us demonstrate the following theorem.

Page 123.

Theorem 3.24. If in the system with the odd bases/bases is given even number A of form $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ with trace S_A, character Δ_A and quantity of incorrect digits λ, then the number, which is obtained as a result of division A into two

$$\frac{A}{2} = (\beta_1, \beta_2, \ldots, \beta_n),$$

it has a trace

$$S_{\frac{A}{2}} = \frac{S_A + \lambda}{2} \pmod{p_n} \qquad (3.79)$$

and a character

$$\Delta_{\frac{A}{2}} = \frac{\xi + \Delta_A - \eta_n - \gamma}{2}, \qquad (3.80)$$

where value ξ and η_n they can be defined as

$$\xi = \begin{cases} 1, & \text{если } S_A + \lambda \text{ нечетное,}(1) \\ 0, & \text{если } S_A + \lambda \text{ четное,}(3) \end{cases} \qquad (3.81)$$

$$\eta_n = \begin{cases} 1, & \text{если } \alpha_n \text{ нечетное}(2) \\ 0, & \text{если } \alpha_n \text{ четное.}(3) \end{cases} \qquad (3.82)$$

Key: (1). if. (2). odd. (3). even.

Proof. Since in view of the condition of theorem A - even number, then has the place

$$A = \frac{A}{2} + \frac{A}{2}. \qquad (3.83)$$

Regarding the trace of sum we have

$$S_A = (S_{\frac{A}{2}} + S_{\frac{A}{2}} - \delta) \pmod{p_n},$$

where δ - number of incorrect pairs in the components/terms/addends A/2 and A/2, i.e., $\delta = \lambda$; hence and it follows (3.79).

For determining the character $\Delta_{\frac{A}{2}}$ let us use the criterion of

overflow for (3.83). In this case, naturally, the overflow cannot take the place

$$\Delta_{\frac{A}{2}} + \Delta_{\frac{A}{2}} + \eta_n - \Delta_A - \xi + \gamma = 0,$$

whence it ensues/escapes/flows out (3.80).

If $S_A + \lambda$ - odd number, then during division $S_{A+\lambda}$ into two for obtaining $S_{\frac{A}{2}}$ it is necessary to add basis/base p_n, which is equivalent to the presence of transition through p_n during addition i.e. $S_{\frac{A}{2}} + S_{\frac{A}{2}}, \xi = 1.$

Page 124.

But if $S_A + \lambda$ - even, then during determination $S_{\frac{A}{2}}$ it completely is divided by two and, therefore, during addition $S_{\frac{A}{2}} + S_{\frac{A}{2}}$ cannot be transition through p_n, i.e. $\xi = 0$. Thus is confirmed validity (3.81).

Concerning η_m, then it also is determined on the parity or oddness α_n. Actually/really, if α_n odd, then for formation/education β_n we add to α_n basis/base p_n and then with addition $\beta_n + \beta_n$ will occur transition through basis/base p_n. Thus is proven the validity of relationship/ratio (3.82).

The absence in the system of even bases/bases creates convenience during the division into 2, but impedes the determination

of parity or oddness of a number.

Let us examine the situation when among the foundations for of system eating an even basis/base. Let for certainty $p_1=2$. then by form of number $A(\alpha_1, \alpha_2, \ldots, \alpha_n)$ it is possible to judge about its parity, namely: with $\alpha_1=1$, number A odd, with $\alpha_1=0$, number A even.

Let us examine even number $A=(0, \alpha_2, \ldots, \alpha_n)$ trace S_A and character Δ_A of which they are known. During division of A into 2 we will obtain number $A/2=(\beta_1, \beta_2, \ldots, \beta_n)$, all digits of which are determined unambiguously, except digit β_1 according to base p_1. For the digit β_1 we obtain an uncertainty/indeterminancy of the type 0/0. Generally speaking digit β_1 can have either a value of 0 or 1. Let us designate through $(A/2)_0$ and $(A/2)_1$, the numbers

$$\left(\frac{A}{2}\right)_0 = (0, \beta_2, \ldots, \beta_n) \text{ со}^{(1)}\text{следом } S^0_{\frac{A}{2}},$$

$$\left(\frac{A}{2}\right)_1 = (1, \beta_2, \ldots, \beta_n) \text{ со следом } S^1_{\frac{A}{2}}.$$

Key: (1). with the trace.

Digit $\alpha_1=0$ can be obtained from the sum $\beta_1+\beta_1$ both with $\beta_1=0$ and with $\beta_1=1$, i.e., from the addition both $2(A/2)_0$ and $2(A/2)_1$. With addition $2(A/2)_0$ the obtained in A digit $\alpha_1=0$ is correct, since it is correct pair (0, 0), while with addition $2(A/2)_1$, this digit incorrect, since pair (1, 1) is incorrect.

Page 125.

The account of this circumstance is reflected in the traces for $(A/2)_0$ and $(A/2)_1$, which can be defined as

$$S_{\frac{A}{2}}^0 = \frac{S_A + \lambda_0}{2} \pmod{p_n},\qquad (3.84)$$

$$S_{\frac{A}{2}}^1 = \frac{S_A + \lambda_0 + 1}{2} \pmod{p_n},\qquad (3.85)$$

where λ_0 - quantity of incorrect digits in the series/row α_2, α_3, ..., α_{n-1}.

In order to establish/install, which of the versions of number $A/2$ is unknown, let us apply the criterion of overflow, moreover let us assume $\Omega=0$, since with multiplication $A/2$ by 2 only true $A/2$ will not derive result from range $[0, \mathcal{P})$.

We investigate the occurring here possibilities. Let us extract the criterion of the overflow

$$2\Delta_{\frac{A}{2}} + \eta_m - \Delta_A - \xi + \gamma = 0.\qquad (3.86)$$

During the analysis of the criterion of overflow we have available the values of values Δ_A, S_A, λ_0, and therefore, to us was known value γ. Let us present $S_A + \lambda_0$ and $S_A + \lambda_0 + 1$ in the form

$$S_A + \lambda_0 = \gamma p_n + \rho_1,$$
$$S_A + \lambda_0 + 1 = \gamma p_n + \rho_2.$$

where $\rho_i < p_n$ - whole non-negative number.

Let us examine the possible cases, after introducing for the convenience the designation

$$\Delta_A^0 = \begin{cases} 1, & \text{(1) если } \Delta_A = 1, \\ 0 & \text{(2) в остальных случаях.} \end{cases}$$

Key: (1). if. (2). in remaining cases.

Case 1. $\Delta_A = 1$

Version 1.1. α_n even, $\gamma - 1$.

If α_n even, then $\eta_n = 0$. In this version the criterion of overflow accepts the form

$$2\Delta_{\frac{A}{2}} - \xi = 0,$$

whence $\xi = \Delta_{\frac{A}{2}} = 0$.

But this means that the unknown quantity has that value $S_A + \lambda_0$ either $_\wedge$ which is even, or the value ρ_1 or ρ_2, which is odd.
$S_A + \lambda_0 + 1,$

Page 126.

The selection of corresponding value $S_A + \lambda_0$ or $S_A + \lambda_0 + 1$ uniquely determines by (3.84) and (3.85) value β_1, namely:

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n - 1) \wedge \gamma \wedge \psi(\rho_2).$$

Here $\psi(x)$ is a function of the parity of number x, defined as

$$\psi(x) = \begin{cases} 1 & \text{если } x - \text{нечетное число,} \quad (2) \\ 0 & \text{если } x - \text{четное число.} \quad (3) \end{cases}$$

Key: (1). if. (2). odd number. (3). even number.

Version 1.2. α_n even, $\gamma=0$.

$$2\Delta_{\frac{A}{2}} - 1 - \xi = 0,$$

The criterion of overflow in this version takes the form

whence possible the unique value ξ and $\Delta_{\frac{A}{2}}$:

$$\xi = \Delta_{\frac{A}{2}} = 1.$$

Therefore, unknown is the number which has $S_A + \lambda_0$ either

$S_A + \lambda_0 + 1$ - odd value, or ρ_1 or ρ_2 odd. Hence

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n - 1) \wedge \bar{\gamma} \wedge \psi(\rho_2).$$

Value β_1, in versions 1.1 and 1.2 can be determined by the general formula

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n - 1) \wedge \psi(\rho_2). \qquad (3.87)$$

Version 1.3. α_n odd, $\gamma=1$.

In this version $\eta_n=1$. condition (3.86) can be rewritten in the form

$$2\Delta_{\frac{A}{2}} - \xi + 1 = 0,$$

whence $\xi=1$, $\Delta_{\frac{A}{2}} = 0$.

Then unknown quantity is that which has $S_A + \lambda_0$ or $S_A + \lambda_0 + 1$ odd and ρ_1 or ρ_2 even, i.e.

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n) \wedge \gamma \wedge \psi(\rho_2 - 1).$$

Version 1.4 α_n odd, $\gamma = 0$.

Page 127.

Condition (3.86) accepts the form

$$2\Delta_{\frac{A}{2}} - \xi = 0,$$

whence $\xi = \Delta_{\frac{A}{2}} = 0$ and in unknown quantity value ρ_1 or ρ_2 even, and therefore, value β_1 can be defined as

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n) \wedge \bar{\gamma} \wedge \psi(\rho_2 - 1).$$

Value β_1 in versions 1.3 and 1.4 can be determined by the general formula

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n) \wedge \psi(\rho_2 - 1). \qquad (3.88)$$

Case of 2. $\Delta_A = 0$.

Version 2.1. α_n even, $\gamma = 1$.

The criterion of overflow will be written as

$$2\Delta_{\frac{A}{2}} - \xi + 1 = 0,$$

whence $\xi = 1$, $\Delta_{\frac{A}{2}} = 0$

and

$$\beta_1 = \bar{\Delta}_A^0 \wedge \psi(\alpha_n - 1) \wedge \gamma \wedge \psi(\rho_2 - 1).$$

Version 2.2 α_n even, $\gamma = 0$.

The criterion of overflow acquires the form

$$2\Delta_{\frac{A}{2}} - \xi = 0,$$

whence $\xi = \Delta_{\frac{A}{2}} = 0$.

Unknown quantity is that which has ρ_1 or ρ_2 - even number, whence

$$\beta_1 = \overline{\Delta}^{\circ}_A \wedge \psi(\alpha_n - 1) \wedge \overline{\gamma} \wedge \psi(\rho_2 - 1).$$

General formula for β_1 in versions 2.1 and 2.2 takes the form

$$\beta_1 = \overline{\Delta}^{\circ}_A \wedge \psi(\alpha_n - 1) \wedge \psi(\rho_2 - 1). \qquad (3.89)$$

Version 2.3 α_n odd, $\gamma = 1$.

Condition (3.86) can be written in the form

$$2\Delta_{\frac{A}{2}} + 2 - \xi = 0,$$

hence $\xi = 0$, $\Delta_{\frac{A}{2}} = -1$.

Therefore, value β_1 can be defined as

$$\beta_1 = \overline{\Delta}_A \wedge \psi(\alpha_n) \wedge \gamma \wedge \psi(\rho_2).$$

Page 128.

Version 2.4. α_n odd, $\gamma = 0$.

Condition (3.86) acquires the form

$$2\Delta_{\frac{A}{2}} + 1 - \xi = 0,$$

whence $\xi = 1$, $\Delta_{\frac{A}{2}} = 0$. Then

$$\beta_1 = \overline{\Delta}_A^0 \wedge \psi(\alpha_n) \wedge \overline{\gamma} \wedge \psi(\rho_2).$$

General formula β_1 for versions 2.3 and 2.4 takes the form

$$\beta_1 = \overline{\Delta}_A^0 \wedge \psi(\alpha_n) \wedge \psi(\rho_2). \qquad (3.90)$$

Case of 3. $\Delta_A = -1$.

Version 3.1. α_n even $\gamma = 1$.

In this version the criterion of overflow acquires the form

$$2\Delta_{\frac{A}{2}} + 2 - \xi = 0,$$

$$^{(1)}\text{откуда } \xi = 0, \; \Delta_{\frac{A}{2}} = -1.$$

Key: (1). whence.

Let us introduce the designation

$$\Delta_A^0 = \begin{cases} 1, ^{(1)}\text{если } \Delta_A = -1, \\ 0 \; ^{(2)}\text{в остальных случаях.} \end{cases}$$

Key: (1). if. (2). in remaining cases.

Then

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n - 1) \wedge \gamma \wedge \psi(\rho_2).$$

Version 3.2 α_n even, $\gamma = 0$.

The criterion of overflow in this version can be written

$$2\Delta_{\frac{A}{2}} + 1 - \xi = 0.$$

Here $\xi = 1, \Delta_{\frac{A}{2}} = 0$.

Hence

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n - 1) \wedge \overline{\gamma} \wedge \psi(\rho_2).$$

General formula for β_1 in versions 3.1 and 3.2 acquires the form

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n - 1) \wedge \psi(\rho_2). \qquad (3.91)$$

Version 3.3. α_n - odd, $\gamma = 1$.

Let us write the form of the criterion of the overflow

$$2\Delta_{\frac{A}{2}} + 3 - \xi = 0,$$

whence $\xi = 1, \Delta_{\frac{A}{2}} = -1$.

Page 129.

To unknown quantity corresponds that of the values ρ_1 or ρ_2, which is even. Hence

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n) \wedge \gamma \wedge \psi(\rho_2 - 1).$$

Version 3.4 α_n odd, $\gamma = 0$.

For the criterion of overflow we obtain the expression

$$2\Delta_{\frac{A}{2}} + 2 - \xi = 0,$$

whence $\xi = 0$, $\Delta_{\frac{A}{2}} = -1$. Then

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n) \wedge \overline{\gamma} \wedge \psi(\rho_2 - 1).$$

In versions 3.3 and 3.4 general formula for β_1 will take the form

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n) \wedge \psi(\rho_2 - 1). \qquad (3.92)$$

The cases examined can be generalized into the following theorem.

Theorem 3.25. If in the system of oases/bases $p_1 = 2$, p_2, p_3, ..., p_n is preset even number $A = (0, \alpha_2, \alpha_3, ..., \alpha_n)$. then in the quotient of the division of number A into 2: $\frac{A}{2} = (\beta_1, \beta_2, ... \beta_n)$, digits β_2, ..., β_n are defined by the step-by-step division of the corresponding digits of dividend into 2, and digit β_1 is defined by the relationship/ratio

$$\beta_1 = \Delta_A^0 \wedge \psi(\alpha_n + \rho_2) \vee \overline{\Delta}_A^0 \wedge \psi(\alpha_n + \rho_2 - 1). \qquad (3.93)$$

where Δ_A^0 is defined as

$$\Delta_A^0 = \begin{cases} 1,^{(1)}\text{если } \Delta_A \text{ }^{(2)}\text{равно } +1 \text{ или}^{(3)} -1, \\ 0,^{(4)}\text{если } \Delta_A \text{ равно нулю.} \end{cases}$$

Key: (1). if. (2). it is equal. (3). or (4). it is equal to zero.

The character of quotient $\Delta_{\frac{A}{2}}$ is determined

$$\Delta_{\frac{A}{2}} = \begin{cases} 1,^{(1)}\text{если } \Delta_A = 1, \quad \psi(\alpha_n) = 0, \gamma = 0, \\ -1,^{(2)}\text{если } \Delta_A = 0, \quad \psi(\alpha_n) = 1, \gamma = 1, \\ ^{(3)}\text{или } \Delta_A = -1, \psi(\alpha_n) = 1, \\ ^{(4)}\text{или } \Delta_A = -1, \psi(\alpha_n) = 0, \gamma = 1, \\ 0 \text{ в остальных случаях.}^{(5)} \end{cases} \qquad (3.94)$$

Key: (1). if. (2). or. (3). In the remaining cases.

and its trace

$$S_{\frac{A}{2}} = \frac{S_A + \lambda_0 + \beta_1}{2}.$$

Page 130.

Proof. Proof is based on obtained previously expressions
(3.87)-(3.92). In this case it is considered that expressions (3.87),
(3.88), (3.91), (3.92) are dedicated to the cases when a_n and ρ_2 -
value of different parity, and in expressions (3.89), (3.90) these
values of identical parity, that also is reflected in (3.93).

Let us examine the methods of determining the parity of a number
when among the bases/bases there are no even ones. Let us introduce
the preliminarily following determination.

Determination. By the formal division of number A into number B
we will understand such process, during which the digits of quotient
are obtained as the result of the step-by-step division of the digits
of divisible/fissionable into the appropriate digits
divider/denominator.

Theorem 3.26. If in the system with the odd bases/bases

$$p_1, p_2, \ldots, p_n$$

is preset number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ with trace S_A, character Δ_A and number of incorrect digits λ and if quotient from the formal division of A into 2

$$\left(\frac{A}{2}\right)_{\bullet} = (\beta_1, \beta_2, \ldots, \beta_n)$$

with trace $S_{\frac{A}{2}}$ and character $\Delta_{\frac{A}{2}}$, then parity or oddness of number A is preset defined by the following relationship/ratio:

$$\psi(A) = \psi(\eta_n - \Delta_A - \xi + \gamma), \qquad (3.95)$$

where values η_n and ξ can be defined as

$$\eta_n = \psi(\alpha_n),$$
$$\xi = \psi(S_A + \lambda). \qquad (3.96)$$

Proof. Since A/2 is obtained by the formal division of number A into 2, then in the case when A odd, quotient of the division exist

$$\frac{A + \mathscr{P}}{2},$$

therefore with the addition of particular, obtained during the formal division of A into 2, with themselves overflow itself it will not be, if the initial number A was even, and overflow will occur, if number A is odd.

Page 131.

In other words

$$\psi(A) = \Omega$$

or

$$\psi(A) = 2\Delta_{\frac{A}{2}} + \eta_n - \Delta_A - \xi + \gamma.$$

Hence

$$\psi(A) - \eta_n + \Delta_A + \xi - \gamma = 2\Delta_{\frac{A}{2}}.$$

The left side of the obtained expression is even, that can be written as

$$\psi(\psi(A) - \eta_n + \Delta_A + \xi - \gamma) = 0,$$

whence and follows the assertion of the theorem

$$\psi(A) = \psi(\eta_n - \Delta_A - \xi + \gamma).$$

In a number of cases when it is necessary to determine value $A/2$, is admissible the use/application of the following method: if the preset number A is even, then searches for value $A/2$, but if number A is odd, then value $(A-1)/2$. In this case the determination of value $A-1/2$ can be organized in such a way that the actual subtraction would not be carried out, but only it was implied. Let us examine the methods of calculation $S_{\frac{A-1}{2}}$ and $\Delta_{\frac{A-1}{2}}$, when they are known S_A, Δ_A, λ_A. Let us introduce the following determination.

Determination. Digit α_i we will call incorrect first-order digit, if pair $(\alpha_i, p_i - 1)$ is incorrect pair, and by correct first-order digit otherwise. A quantity of incorrect first-order digits in number A we will indicate through λ_1. Digit $\alpha_i - 1$ we will call incorrect second-order digit, if pair $\left(\frac{\alpha_i - 1}{2}, \frac{\alpha_i - 1}{2}\right)$ is incorrect pair, and by correct second-order digit otherwise. A quantity of incorrect second-order digits in a number we will indicate through λ_2.

Let be preset odd number A. Then we can write

$$A-1 = A+(\mathscr{P}-1)$$

and

$$S_{A-1} = S_A + S_{\mathscr{P}-1} - \lambda_1$$

Page 132.

Here $S_{\mathscr{P}-1}$ with the selected bases/bases is a constant value. Then for $S_{\frac{A-1}{2}}$ is correct the expression

$$S_{\frac{A-1}{2}} = \frac{S_A + S_{\mathscr{P}-1} - \lambda_1 + \lambda_2}{2} . \qquad (3.97)$$

Concerning $\Delta_{\frac{A-1}{2}}$, let us compute first Δ_{A-1}. Taking into account that $\Delta_{\mathscr{P}-1} = 0$ and that with addition $A+(\mathscr{P}-1)$ has the place overflow, we will obtain

$$\Delta_A + \eta_n - \Delta_{A-1} - \xi + \gamma = 1,$$

whence

$$\Delta_{A-1} = \Delta_A + \eta_n - \xi + \gamma - 1,$$

or, by taking into account (3.80) and (3.96), we will obtain

$$\Delta_{\frac{A-1}{2}} =$$
$$= \frac{\psi(S_A + S_{\mathscr{P}-1} - \lambda_1 + \lambda_2) + \Delta_A + \eta_n - \xi + \gamma - 1 - \psi((\alpha_n + p_n - 1)(\bmod p_n))}{2} .$$

If $\alpha_n \neq 0$, then $\eta_n = 1$ and

$$\Delta_{\frac{A-1}{2}} = \frac{\psi(S_A + S_{\mathscr{P}-1} - \lambda_1 + \lambda_2) + \Delta_A - \xi + \gamma - \psi(\alpha_n - 1)}{2} .$$

But if $\alpha_n = 0$, then

$$\Delta_{\frac{A-1}{2}} = \frac{\psi(S_A + S_{\mathscr{P}-1} - \lambda_1 + \lambda_2) + \Delta_A - \xi + \gamma - 1}{2} .$$

Thus, is examined a question about the division of number A into 2, which corresponds to the shift/shear of a binary positional number to one digit to the right.

Let us examine now a question about the division into 4, which corresponds to the shift/shear of a positional number to two digits to the right. Let in the system with the odd bases/bases be is preset the multiple 4 number A with trace S_A and character Δ_A. Let it be further by step-by-step division it is obtained

$$\frac{A}{4} = (\widetilde{\gamma}_1, \widetilde{\gamma}_2, \ldots, \widetilde{\gamma}_n).$$

Since among the bases/bases there are no even ones, it is possible to say that via of A/4 indicated it is unambiguously determined.

Page 133.

If we designate through λ' value

$$\lambda' = \delta\left(\frac{A}{4}, \frac{A}{4}\right) + \delta\left(2\frac{A}{4}, \frac{A}{4}\right) + \delta\left(3\frac{A}{4}, \frac{A}{4}\right),$$

where δ - number of incorrect pairs of digits in the appropriate operands of sum, then we can write for $S_{\frac{A}{4}}$ the expression

$$S_{\frac{A}{4}} = \frac{S_A + \lambda'}{4}. \qquad (3.98)$$

Concerning $\Delta_{\frac{A}{4}}$, then it is determined from the condition so that A/4, multiplied by 4, would not leave range $[0, \mathscr{P})$, namely:

$$4\Delta_{\frac{A}{4}} + \eta_n(\widetilde{\gamma}_n, \widetilde{\gamma}_n) + \eta_n(2\widetilde{\gamma}_n, \widetilde{\gamma}_n) + \eta_n(3\widetilde{\gamma}_n, \widetilde{\gamma}_n) - \Delta_A -$$
$$-\xi\left(\frac{A}{4}, \frac{A}{4}\right) - \xi\left(2\frac{A}{4}, \frac{A}{4}\right) - \xi\left(3\frac{A}{4}, \frac{A}{4}\right) + \gamma\left(\frac{A}{4}, \frac{A}{4}\right) +$$
$$+\gamma\left(2\frac{A}{4}, \frac{A}{4}\right) + \gamma\left(3\frac{A}{4}, \frac{A}{4}\right) = 0;$$

whence

$$\Delta_{\frac{A}{4}} = \frac{1}{4} \left\{ \Delta_A - (\eta_n(\widetilde{\gamma}_n, \widetilde{\gamma}_n) + \eta_n(2\widetilde{\gamma}_n, \widetilde{\gamma}_n) + \eta_n(3\widetilde{\gamma}_n, \widetilde{\gamma}_n)) + \right.$$

$$+ \xi\left(\frac{A}{4}, \frac{A}{4}\right) + \xi\left(2\frac{A}{4}, \frac{A}{4}\right) + \xi\left(3\frac{A}{4}, \frac{A}{4}\right) - \left(\gamma\left(\frac{A}{4}, \frac{A}{4}\right) + \right.$$

$$\left. \left. + \gamma\left(2\frac{A}{4}, \frac{A}{4}\right) + \gamma\left(3\frac{A}{4}, \frac{A}{4}\right)\right) \right\} . \qquad (3.99)$$

From (3.99) it is evident that character $\Delta_{\frac{A}{4}}$ can be equal to unity in one case when all ξ are equal to unity, and all η_n and γ are equal to zero and $\Delta_A = 1$. That as $\widetilde{\gamma}_n$ is quotient $\frac{\alpha_n}{4}$, then

$$\eta_n(\widetilde{\gamma}_n, \widetilde{\gamma}_n) = 0, \ \eta_n(2\widetilde{\gamma}_n, \widetilde{\gamma}_n) = 0, \ \eta_n(3\widetilde{\gamma}_n, \widetilde{\gamma}_n) = 0$$

will occur only when α_n is multiple four. All ξ will be equal to unity only if value $S_A + \lambda' + 3\rho_n$ is multiple four.

Let us introduce the function $\mu(x)$, determined by the conditions

$$\mu(x) = \begin{cases} 0, \text{ если } x \text{ кратно четырем.} (\cdot) \\ 1, \text{ если } x \text{ некратно четырем} (\cdot) \end{cases}$$

Key: (1). if x is multiple four. (2). if x it is nonmultiple four.

Page 134.

Then can be formulated the following theorem.

Theorem 3.27. If in the system with odd bases/bases $p_1, p_2, \ldots, p_n$ is preset number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ with trace S_A and character Δ_A, that separates completely into four, and if quotient of the division of A into four $\frac{A}{4} = (\tilde{\gamma}_1, \tilde{\gamma}_2, \ldots, \tilde{\gamma}_n)$ with trace $S_{\frac{A}{4}}$ and character $\Delta_{\frac{A}{4}}$, then for $p_n = 4k + 1$, where k - whole non-negative number:

value $\Delta_{\frac{A}{4}}$ is determined from the expression

$$\Delta_{\frac{A}{4}} = \overline{\mu(\alpha_n)} \wedge \overline{\mu(S_A + \lambda' + 3)} \wedge \Delta_A, \qquad (3.100)$$

but for $p_n = 4k - 1$ - from the expression

$$\Delta_{\frac{A}{4}} = \overline{\mu(\alpha_n)} \wedge \overline{\mu(S_A + \lambda' + 1)} \wedge \Delta_A. \qquad (3.101)$$

Proof. Let us first of all focus attention on the fact that any odd basis/base can be expressed in the form

$$p_i \equiv \theta \pmod 4,$$

where θ can have a value of 1 or 3. But then odd basis/base can take either form $p_i = 4k + 1$, or form $p_i = 4k - 1$. Let us further note that the condition

$$\alpha_n \equiv 0 \pmod 4 \qquad (3.102)$$

is necessary and sufficient so that would have the place

$$\eta_n(\tilde{\gamma}_n, \tilde{\gamma}_n) = \eta_n(2\tilde{\gamma}_n, \tilde{\gamma}_n) = \eta_n(3\tilde{\gamma}_n, \tilde{\gamma}_n) = 0. \qquad (3.103)$$

Actually/really, let (3.103) have the place. This means that with addition $\tilde{\gamma}_n$ with itself four times itself it was not transition through basis/base p_n. In other words,

$$\alpha_n = 4\tilde{\gamma}_n$$

or

$$\alpha_n \equiv 0 \,(\mathrm{mod}\,4).$$

let it be now correct (3.102). let us assume that (3.103) it does not

have place, i.e., with the addition of very with themselves $\tilde{\gamma}_n$

occurred transitions through the basis/base, i.e.

$$\alpha_n = 4\tilde{\gamma}_n - l p_n.$$

where l - number of transitions through basis/base p_n.

Page 135.

Since $p_n = 4k \pm 1$, then $\alpha_n = 4\tilde{\gamma}_n - 4lk \pm l$, whence

$$\alpha_n \equiv l \,(\mathrm{mod}\ 4)$$

or

$$\alpha_n \equiv (4 - l) \,(\mathrm{mod}\ 4).$$

But this contradicts our assumption (3.102). Further, the expression

$$\mu(S_A + \lambda' + 3p_n) = 0$$

for basis/base $p_n = 4k + 1$ is converted into the expression

$$\mu(S_A + \lambda' + 3) = 0,$$

and for $p_n = 4k - 1$ - to the form

$$\mu(S_A + \lambda' + 1) = 0.$$

Thus is established/installed the validity of relationships

(3.100) and (3.101), that constitute the assertion of theorem.

Let us examine now the situation when one of the basis of system is equal to four. Let $p_1 = 4$. Then the multiplicity of number A four leads to the value $\alpha_1 = 0$. Let us designate quotient of the division of A into 4

$$\frac{A}{4} = (\tilde{\gamma}_1, \tilde{\gamma}_2, \ldots, \tilde{\gamma}_n).$$

For the digit γ_1 we will obtain an uncertainty/indeterminancy of the type 0/0. Are possible four value of digit $\tilde{\gamma}_1$: 0, 1, 2, 3. Let us designate through $\left(\frac{A}{4}\right)^0$, $\left(\frac{A}{4}\right)^1$, $\left(\frac{A}{4}\right)^2$, $\left(\frac{A}{4}\right)^3$ the quotients of the division of A into 4 with the appropriate value of digit $\tilde{\gamma}_1$. In this case our task it is to correct carry out a selection of the corresponding digit $\tilde{\gamma}_1$.

Let us demonstrate the preliminarily following theorem.

Page 136.

Theorem 3.28. If in the system with bases/bases $p_1 = 4$, $p_2, \ldots, p_n$ is preset on basis/base p_1 the pair of digits $(\tilde{\gamma}_1, \tilde{\gamma}_1)$, then with base p_n, equal to

$$p_n = 4k + 1,$$

besides the incorrect pairs, determined in general, will be incorrect also following pairs:

ω) при $m_1 = 1$ пары (2, 3) и (3, 3),   (3.104)

② при $m_1 = 3$ пары (1, 1) и (1, 2),   (3.105)

(3) при основании p_n, равном

$$p_n = 4k - 1,$$

ω) при $m_1 = 1$ пары (1, 1) и (1, 2),   (3.106)

② при $m_1 = 3$ пары (2, 3) и (3, 3).   (3.107)

Key: (1). with. (2). pair. (3). with basis/base p_n, equal.

Proof. With $m_1 = 1$ the ranks of minimum pseudo-orthogonal numbers

for any γ_1 are equal to unity. Then the minimum trace of a number (1,

0, ..., 0, S_1^*) is defined as

$$S_1^* = \left[\frac{4-1}{4}p_n\right] + 1 = \left[\frac{3}{4}p_n\right] + 1.$$

For a number (2, 0, ..., 0, S_2^*) we will obtain

$$S_2^* = \left[\frac{4-2}{4}p_n\right] + 1 = \left[\frac{1}{2}p_n\right] + 1.$$

For number (3, 0, ..., 0, S_3^*) we will have

$$S_3^* = \left[\frac{4-3}{4}p_n\right] + 1 = \left[\frac{1}{4}p_n\right] + 1.$$

Let us evaluate correctness of pair (2, 3) for basis/base p_n of the

form

$$p_n = 4k + 1.$$

Here

$$S_1^* = 3k + 1, \ S_2^* = 2k + 1, \ S_3^* = k + 1,$$

then

$$S_2^* + S_3^* = 3k + 2$$

or

$$S_2^* + S_3^* = S_1^* + 1,$$

i.e. pair (2, 3) is incorrect.

For the same basis/base let us examine pair (3, 3)

$$S_3^* + S_3^* = 2k + 2$$

or

$$S_3^* + S_3^* = S_2^* + 1,$$

i.e. (3.3) it is incorrect pair. We demonstrated (3.104).

Let us now move on to proof (3.106). $p_n = 4k - 1$. Then $S_1^* = 3k$, $S_2^* = 2k$, $S_3^* = k$.

Page 137.

Let us examine pair (1, 1)

$$S_1^* + S_1^* = 6k = 2k + 1$$

and

$$S_1^* + S_1^* = S_2^* + 1,$$

i.e. (1, 1) - incorrect pair.

For pair (1, 2) we will have

$$S_1^* + S_2^* = k + 1$$

and

$$S_1^* + S_2^* = S_3^* + 1,$$

i.e. pair (1, 2) also incorrect. To these we demonstrated (3.106).

Let us switch over to value of $m_1=3$. In this case for a number $(1, 0, \ldots, 0, S_1*)$ we have a rank $r=1$ and

$$S_1^* = \left[\frac{4-3}{4} p_n\right] + 1 = \left[\frac{1}{4} p_n\right] + 1.$$

For a number $(2, 0, \ldots, 0, S_2*)$ we will obtain rank $r=2$ and

$$S_2^* = \left[\frac{8-6}{4} p_n\right] + 1 = \left[\frac{1}{2} p_n\right] + 1.$$

For a number $(3, 0, \ldots, 0, S_3)$ rank $r=3$ and

$$S_3^* = \left[\frac{12-9}{4} p_n\right] + 1 = \left[\frac{3}{4} p_n\right] + 1.$$

Let $p_n=4k+1$. Then $S_1*=k+1$, $S_2*=2k+1$, $S_3*=3k+1$.

Let us examine pair $(1, 1)$. For it

$$S_1^* + S_1^* = 2k+2$$

and

$$S_?^* + S_1^* = S_2^* + 1,$$

i.e. $(1, 1)$ - incorrect pair.

Let us take pair $(1, 2)$. For it

$$S_1^* + S_2^* = 3k+2$$

and

$$S_1^* + S_2^* = S_3^* + 1,$$

i.e. $(1, 2)$ - also incorrect pair. Thereby is proved validity (3.105).

Let us take now $p_n = 4k-1$. Then $S_1{*}{=}k$, $S_2{*}{=}2k$, $S_3{*}{=}3k$. Let us examine pair (2, 3). For it

$$S_2^{*} + S_3^{*} = 5k = k + 1.$$

pair (2, 3) is incorrect, since

$$S_2^{*} + S_3^{*} = S_1^{*} + 1.$$

Page 138.

For pair (3, 3) we have

$$S_3^* + S_3^* = 6k = 2k + 1.$$

This pair also is incorrect, since

$$S_3^* + S_3^* = S_2^* + 1.$$

By this is proved assertion (3.107) of theorem.

Corollary 1. If number A is divided completely by 4, then during the calculation of value $\tilde{\lambda}_i$

$$\tilde{\lambda}_i = \delta\left(\frac{A}{4}, \frac{A}{4}\right) + \delta\left(2\frac{A}{4}, \frac{A}{4}\right) + \delta\left(3\frac{A}{4}, \frac{A}{4}\right).$$
$$i = 0, 1, 2, 3,$$

for each of the alternative expressions $\left(\frac{A}{4}\right)^0$, $\left(\frac{A}{4}\right)^1$, $\left(\frac{A}{4}\right)^2$, $\left(\frac{A}{4}\right)^3$ among $\tilde{\lambda}_0$, $\tilde{\lambda}_1$, $\tilde{\lambda}_2$, $\tilde{\lambda}_3$ there are no identical ones with respect to value, and maximum value are $(\tilde{\lambda}_i)_{max} = 3$.

Proof. According to theorem 3.19 any pair of digits, which gives in sum of $p_1 = 4$, is incorrect, i.e., always incorrect are pairs (1, 3), (2, 2), (3, 1).

Let us consider now each of $\widetilde{\lambda}_i$ $(i = 0, 1, 2, 3)$. Let us note that $\widetilde{\lambda}_0 = 0$. Then values $\widetilde{\lambda}_i$ are defined as

$$\widetilde{\lambda}_1 = \delta(1, 1) + \delta(2, 1) + \delta(3, 1),$$
$$\widetilde{\lambda}_2 = \delta(2, 2) + \delta(0, 2) + \delta(2, 2),$$
$$\widetilde{\lambda}_3 = \delta(3, 3) + \delta(2, 3) + \delta(1, 3)$$

and it is possible to make table values $\widetilde{\lambda}_i$.

For $m_1 = 1$ we will obtain

p_n $\widetilde{\lambda}_i$	$4k + 1$	$4k - 1$
$\widetilde{\lambda}_0$	0	0
$\widetilde{\lambda}_1$	1	3
$\widetilde{\lambda}_2$	2	2
$\widetilde{\lambda}_3$	3	1

and for $m_1 = 3$ we will obtain

p_n $\widetilde{\lambda}_i$	$4k + 1$	$4k - 1$
$\widetilde{\lambda}_0$	0	0
$\widetilde{\lambda}_1$	3	1
$\widetilde{\lambda}_2$	2	2
$\widetilde{\lambda}_3$	1	3

Page 139.

From the comparison of the obtained values for $\widetilde{\lambda}_0$, $\widetilde{\lambda}_1$, $\widetilde{\lambda}_2$, $\widetilde{\lambda}_3$

escape/ensue the formulated in corollary 1 assertions.

Corollary 2. If number A is divided completely by 4, then among the traces

$$S_{\frac{A}{4}}^{i} = \frac{S_A + \tilde{\lambda}_i + \lambda_0}{4} = \frac{S_A^i}{4}$$

of alternative expressions $\left(\frac{A}{4}\right)^0$, $\left(\frac{A}{4}\right)^1$, $\left(\frac{A}{4}\right)^2$, $\left(\frac{A}{4}\right)^3$ there are no identical ones with respect to value, and maximum difference $S_A^{i_1} - S_A^{i_2}$ is equal to three.

Proof. This corollary directly escape/ensues from previous, since the absence of equal values among $\tilde{\lambda}_i$ does not allow/assume equal values among S_A^i, but limitedness $(\tilde{\lambda}_i)_{max}$ by digit 3 determines and

$$\max (S_A^{i_1} - S_A^{i_2}) = \max (\tilde{\lambda}_{i_1} - \tilde{\lambda}_{i_2}) = 3.$$

From this corollary it follows that each digit $\tilde{\gamma}_1$ answers its value S_A^i moreover it is possible to place digits $\tilde{\gamma}_1$ in such sequence that S_A^i for the adjacent digits would differ from each other by unit. Concrete/specific/actual location in different cases can be determined by the following table.

S_A^i	$m_1 = 1$		$m_1 = 3$	
	$p_n = 4k - 1$	$p_n = 4k + 1$	$p_n = 4k - 1$	$p_n = 4k + 1$
$S_A + \lambda_0$	$\widetilde{\gamma}_1 = 0$	$\widetilde{\gamma}_1 = 0$	$\widetilde{\gamma}_1 = 0$	$\widetilde{\gamma}_1 = 0$
$S_A + \lambda_0 + 1$	$\widetilde{\gamma}_1 = 3$	$\widetilde{\gamma}_1 = 1$	$\widetilde{\gamma}_1 = 1$	$\widetilde{\gamma}_1 = 3$
$S_A + \lambda_0 + 2$	$\widetilde{\gamma}_1 = 2$	$\widetilde{\gamma}_1 = 2$	$\widetilde{\gamma}_1 = 2$	$\widetilde{\gamma}_1 = 2$
$S_A + \lambda_0 + 3$	$\widetilde{\gamma}_1 = 1$	$\widetilde{\gamma}_1 = 3$	$\widetilde{\gamma}_1 = 3$	$\widetilde{\gamma}_1 = 1$

Page 140. Now it is possible to already indicate path for the selection of necessary digit $\widetilde{\gamma}_1$. True digit will be that $\widetilde{\gamma}_1$ for which the sum

$$\left(\frac{A}{4}\right)^i + \left(\frac{A}{4}\right)^i + \left(\frac{A}{4}\right)^i + \left(\frac{A}{4}\right)^i = 4\left(\frac{A}{4}\right)^i = A$$

it is found in the range $[0, \mathcal{P})$. Consequently, it is possible to use the condition of nonappearance from the range $[0, \mathcal{P})$ of the sum of 4 components/terms/addends, which let us register in the form

$$4\Delta_{\frac{A}{4}} + \eta_n(\widetilde{\gamma}_n, \widetilde{\gamma}_n) + \eta_n(2\widetilde{\gamma}_n, \widetilde{\gamma}_n) + \eta_n(3\widetilde{\gamma}_n, \widetilde{\gamma}_n) -$$
$$-\Delta_A - \xi\left(\left(\frac{A}{4}\right)^i, \left(\frac{A}{4}\right)^i\right) - \xi\left(\left(\frac{2A}{4}\right)^i, \left(\frac{A}{4}\right)^i\right) -$$
$$-\xi\left(\left(\frac{3A}{4}\right)^i, \left(\frac{A}{4}\right)^i\right) + \nu\left(\left(\frac{A}{4}\right)^i, \left(\frac{A}{4}\right)^i\right) +$$
$$+\nu\left(\left(\frac{2A}{4}\right)^i, \left(\frac{A}{4}\right)^i\right) + \nu\left(\left(\frac{3A}{4}\right)^i, \left(\frac{A}{4}\right)^i\right) = 0.$$

Let in the system with bases/bases $p_1 = 2, p_2, \ldots, p_n$ number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ be divided completely by four.

Then for result $\frac{A}{4} = (\widetilde{\gamma}_1, \widetilde{\gamma}_2, \ldots, \widetilde{\gamma}_n)$, in which digits $\widetilde{\gamma}_2, \widetilde{\gamma}_3, \ldots, \widetilde{\gamma}_n$ are

obtained by the step-by-step division of digits $\alpha_2, \alpha_3, \ldots, \alpha_n$ into four, can seem two possibilities: $\widetilde{\gamma}_1 = 0$ or $\widetilde{\gamma}_1 = 1$. If $\widetilde{\gamma}_1 = 0$, then a number λ' - the total quantity of incorrect pairs, which appear during calculation A as the sums

$$\left\{ \left(\frac{A}{4} + \frac{A}{4} \right) + \frac{A}{4} \right\} + \frac{A}{4} .$$

will be calculated on the basis of digits A, where zero in digit p_1 will be considered as the correct digit, since it will supplement no changes in value λ_0, calculated or the remaining digits.

Page 141.

But if $\widetilde{\gamma}_1 = 1$, then, obviously, λ' must be calculated on the digits of remaining bases/bases (besides p_1) with addition 2, since (1, 1) it is incorrect pair and its participation in the components/terms/addends gives 2 incorrect pairs. Thus, in the case of $p_1 = 2$

$$S^0_{\frac{A}{4}} = \frac{S_A - \lambda_0}{4}$$

or

$$S^1_{\frac{A}{4}} = \frac{S_A + \lambda_0 + 2}{4} .$$

§3.9. Division into the fixed/recorded number.

Until now, we examined the simplest case of division, namely when dividend completely was divided into the divider/denominator. However, in the general case the division represents one of the most

labor-consuming arithmetic operations.

Even in the digital computers, which work in the positional
system of calculation (for example, in the binary), the operation of
division will stand apart and the time of its execution
approximately/exemplarily by an order higher than time of the
execution of the majority of elementary operations.

In the system of residual classes the difficulties of division
are aggravated by the fact that this operation in general is not
"residual", i.e., the digit of quotient on the independent foundation
is no longer determined only by the digits of dividend and
divider/denominator on this basis/base, but it requires in one or the
other form of information about the values of dividend and
divider/denominator as a whole.

In general the division of number A into constant d should be
distinguished two possibilities:

- when d it is not the basis of system and

- when d it enters into the system of bases/bases.

Of the first case the difficulty consists of the establishment

of the very fact of fissionability A on d or, which is the same thing, in the reduction of a number to the nearest to it number A', which separates completely into d. Division itself can be produced step-by-step.

In the second case easily is determined, does share A on d, also easily is determined the near to A number A', which separates completely into d, but the determination of the digit of quotient from basis/base $p_i = d$ requires the disclosure/expansion of uncertainty/indeterminancy, for which appears the need for the enlistment of information about entire number.

Page 142.

Let us consider in more detail the case, when d is not radix, i.e., $d = (\delta_1, \delta_2, \ldots, \delta_n)$. The formal quotient, which is obtained during the division of number A into d,

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$$

can be registered in the following form:

$$\left(\frac{A}{d}\right)_\Phi = \left(\frac{\alpha_1 + k_1 p_1}{\delta_1}, \frac{\alpha_2 + k_2 p_2}{\delta_2}, \ldots, \frac{\alpha_n + k_n p_n}{\delta_n}\right),$$

where $k_i = 0, 1, 2, \ldots, p_i - 1$ $(i = 1, 2, \ldots, n)$ - non-negative integer, such, which $\alpha_i + k_i p_i$ completely is divided into δ_i.

If we through M designate unknown particular, then number A can be represented in the form A=Md+t (t<d), then formal quotient is equal

$$\left(\frac{A}{d}\right)_\phi = \frac{A+k\mathcal{P}}{d} = M + \frac{t+k\mathcal{P}}{d},$$

where k - whole non-negative number.

Hence

$$M = \left(\frac{A}{d}\right)_\phi - \frac{t+k\mathcal{P}}{d}. \qquad (3.108)$$

In the case small d (tentatively $d < p_n$)this method can be considered as the algorithm of division into d. In this case must be withstood the following sequence of operations:

1. Is determined value

$$Q = \left(\frac{A}{d}\right)_\phi = (\alpha_1^{(\phi)}, \alpha_2^{(\phi)}, \ldots, \alpha_n^{(\phi)})$$

by the step-by-step division of A into d.

2. Is determined minimum trace S_Q^* of number Q and it is computed

$$m_n(\alpha_n^{(\phi)} - S_Q^*) \ (\mathrm{mod}\, p_n).$$

3. On $\alpha_n^{(\phi)} - S_Q^*$ is determined number $R = (r_1, r_2, \ldots, r_n)$, which is subtracted from Q, forming M.

Let us give the examples, which illustrate the realization of the algorithm of division examined.

Let us select for this purpose the standardized/normalized system with the bases/bases: $p_1=2$, $p_2=5$, $p_3=7$, $p_4=23$, by range $P=1610$ and by the orthogonal bases: $B_1=805$, $B_2=966$, $B_3=1380$, $B_4=70$.

Page 143.

Let us compute the table of constants R for the division into $d=11$. Constants R are found from the following considerations: is examined near integer to value $\frac{P}{d}=\frac{1610}{11}=146.36\ldots$,   i.e., $R_1=147=(1, 2, 0, 9)$. Here value $\frac{P}{d}$ is rounded off to the large side, since in (3.108) will cost minus sign. Further, we find near integer to $\frac{2P}{d}=292.73\ldots$,   i.e., $R_2=293$ (1, 3, 6, 17) and so forth if is known value $(\alpha_n^\phi-S_Q^\circ)(\mathrm{mod}\, p_n)$. then this it means that is known the interval in which is located number Q. In this case the remainder/residue from subtraction $k\frac{P}{d}$ from Q cannot exceed $\frac{P}{d}$ and in a number of cases it is possible to obtain ambiguity, since both the difference $Q-k\frac{P}{d}$ and difference $Q-(k+1)\frac{P}{d}$ can give remainders/residues less than $\frac{P}{d}$ in the dependence on the value of number A. Let us designate the second possible constant through R', and the remainder/residue, which is obtained in this case, through t'. Then for determining the constants from values $\alpha_n^{(\phi)}-S_Q^\circ$ there can be suggested the following Table.

$\alpha_n^{(\Phi)} - S_Q^*$	R	R'	t	t'
0	0	0	0	0
1	0	0	0	0
2	0	(1, 2, 0, 9)	0	7
3	(1, 2, 0, 9)	0	7	0
4	(1, 2, 0, 9)	(1, 3, 6, 17)	7	3
5	(1, 3, 6, 17)	0	3	0
6	(0, 0, 6, 3)	0	10	0
7	(0, 0, 6, 3)	0	10	0
8	(0, 0, 6, 3)	(0, 1, 5, 11)	10	6
9	(0, 1, 5, 11)	0	6	0
10	(0, 1, 5, 11)	(0, 2, 4, 19)	6	2
11	(0, 2, 4, 19)	0	2	0
12	(0, 2, 4, 19)	(1, 4, 4, 5)	2	9
13	(1, 4, 4, 5)	0	9	0
14	(1, 4, 4, 5)	(1, 0, 3, 13)	9	5
15	(1, 0, 3, 13)	0	5	0
16	(1, 0, 3, 13)	(1, 1, 2, 21)	5	1
17	(1, 1, 2, 21)	0	1	0
18	(1, 1, 2, 21)	(0, 3, 2, 7)	1	8
19	(0, 3, 2, 7)	0	8	0
20	(0, 3, 2, 7)	0	8	0
21	(0, 4, 1, 15)	0	4	0
22	(0, 4, 1, 15)	0	4	0

Page 144.

If A is such, that $\alpha_n^{(\Phi)} - S_Q^*$ it does not bring to single-valued P, then division undergoes A-t', from it is computed $Q' = \left(\frac{A - t'}{d}\right)_\Phi$ and then $\alpha_n^{(\Phi)} - S_Q^*$ gives either t=0 or t=4, which already makes it possible to unambiguously determine R and, therefore, M.

Example. To divide A=(0, 4, 2, 10) into d=(1, 1, 4, 11).

1. It is computed

$$Q = \left(\frac{A}{d}\right)_\Phi = \frac{(0, 4, 2, 10)}{(1, 1, 4, 11)} = (0, 4, 4, 3).$$

2. It is computed

$$\alpha_n^{(\Phi)} - S_Q^* = 3 - 4 \,(\text{mod } 23) = 22.$$

3. In Table through $\alpha_n^{(\phi)} - S_Q^*$ we find R=(0, 4, 1, 15), then

$$M = (0, 4, 4, 3) - (0, 4, 1, 15) = (0, 0, 3, 11).$$

Example. To divide A=(1, 1, 5, 7) into d=(1, 1, 4, 11).

1. It is computed

$$Q = \left(\frac{A}{d}\right)_\phi = \frac{(1, 1, 5, 7)}{(1, 1, 4, 11)} = (1, 1, 3, 9).$$

2. It is computed

$$\alpha_n^{(\phi)} - S_Q^* = 9 - 8 = 1.$$

3. In table we find R=(0, 0, 0, 0), whence M=(1, 1, 3, 9).

An example. To divide A=(1, 2, 4, 1) into d=(1, 1, 4, 11).

1. It is computed

$$Q = \left(\frac{A}{d}\right)_\phi = \frac{(1, 2, 4, 1)}{(1, 1, 4, 11)} = (1, 2, 1, 21).$$

2. It is computed

$$\alpha_n^{(\phi)} - S_Q^* = 21 - 11 = 10.$$

3. In Table we find R=(0, 1, 5, 11), R'=(0, 2, 4, 19), t=6, t'=2.

Here arose alternative, we form

$$. A - t' = (1, 0, 2, 22) \text{ and } Q' = \frac{(1, 0, 2, 22)}{(1, 1, 4, 11)} = (1, 0, 4, 2).$$

Is computed $\alpha_n^{(\phi)} - S_Q^* = 2 - 2 = 0.$ Significant digit t'=2 and then M=(1,

0, 4, 2).

Note. In a latter/last example was computed Q' as the formal quotient A-t'/d. In reality the same result will be obtained simply by subtraction Q-F'.

Page 145.

Let us consider the now more general case of dividing the number A into the product of the whole non-negative numbers D

$$D = d_1 d_2 \ldots d_k,$$

where everything d_i $(i = 1, 2, \ldots, k)$ — mutually prime numbers. Division into D is produced on the basis of the following theorem.

Theorem 3.29. (about the division into the product of numbers). If in the system with range $\mathscr{P}$ is preset number A and is preset k of mutually prime whole non-negative numbers $d_1, d_2, \ldots, d_k$, then always it is possible to select the independent of A integers

$$\mu_1, \mu_2, \ldots, \mu_k,$$

such, that occurs the relationship/ratio

$$\frac{\bar{A}}{d_1 d_2 \ldots d_k} = \mu_1 l_1 + \mu_2 l_2 + \ldots + \mu_k l_k, \qquad (3.109)$$

where l_i are the single quotient:

$$l_i = \frac{A}{d_i} \quad (i = 1, 2, \ldots, k)$$

or, that the same

$$\frac{1}{d_1 d_2 \ldots d_k} = \frac{\mu_1}{d_1} + \frac{\mu_2}{d_2} + \ldots + \frac{\mu_k}{d_k}. \qquad (3.110)$$

Proof. Let us consider case of k=2, when there are two cofactors d_1 and d_2. Then (3.110) is registered as

$$\frac{1}{d_1 d_2} = \frac{\mu_1}{d_1} + \frac{\mu_2}{d_2} \quad \text{or} \quad \mu_1 d_2 + \mu_2 d_1 = 1. \quad (3.111)$$

But since d_1 and d_2 - mutually prime whole non-negative numbers, then always can be found integers μ_1 and μ_2, independent of A, such, which takes place (3.111).

Let us further use the method of induction. Let the theorem be accurate for s cofactors. Let us show that it is accurate for s+1 cofactors. In fact, let us show that

$$\frac{v}{d_1 d_2 \ldots d_s} + \frac{\mu_{s+1}}{d_{s+1}} = \frac{1}{d_1 d_2 \ldots d_{s+1}},$$

where v - integer.

For this must occur the equality

$$v d_{s+1} + \mu_{s+1} \ (d_1 d_2 \ldots d_s) = 1,$$

or, which is the same thing,

$$v d_{s+1} + \mu_{s+1} \ (d_1 d_2 \ldots d_s) \equiv 1 \ (\text{mod } \mathcal{P}).$$

Page 146.

For reasons, presented above, latter/last equality always

occurs, that also proves theorem.

Observation. The accuracy of expression (3.109) is determined by the accuracy of the entering it single quotients. If single quotients are computed approximately, then final result is approximate.

Example. In the system with the basis/bases: $p_1=2$, $p_2=5$, $p_3=7$, $p_4=23$, as the single dividers/denominators let us take $d_1=11=(1, 1, 4, 11)$, $d_2=13=(1, 3, 6, 13)$. In this case divider/denominator D will be $D=d_1d_2=143$, and equality (3.110) will take the form

$$\frac{1}{143}=\frac{\mu_1}{11}+\frac{\mu_2}{13},$$

whence $\mu_1=-5$, $\mu_2=6$.

Let us divide number $A=884=(0, 4, 2, 10)$ into $D=143=(1, 3, 3, 5)$. Let us find the preliminarily single quotients

$$\frac{A}{11}=(0, 0, 3, 11), \quad \frac{A}{13}=(0, 3, 5, 22).$$

Then

$$\frac{A}{143}=-5\left(\frac{A}{11}\right)+6\left(\frac{A}{13}\right)=$$
$$=-(0, 0, 1, 9)+(0, 3, 2, 17)=(0, 3, 1, 8)=8.$$

Results it was obtained inaccurate, since the single quotients were calculated approximately. Considerably better it would be to take $\mu_1=1/2$, $\mu_2=-1/2$, i.e., proceed from the identity

$$\frac{1}{2\cdot11}-\frac{1}{2\cdot13}=\frac{1}{11\cdot13}.$$

Then

$$\frac{A}{143}=\frac{(0, 0, 3, 11)-(0, 3, 5, 22)}{(0, 2, 2, 2)}=(0, 1, 6, 6)=6.$$

This result more exactly approaches number $A/143$ and differs from previous by two units, but in this case μ_1 and μ_2 they are fractional numbers.

§3.10. Division into the basis of system.

Let us now move on to the examination of the division of number A into one of the basis p_i of system with bases/bases p_1, p_2, ..., p_n.

Page 147.

Assume we should divide number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ on p_i (one of the basis of system). Without the loss of generality it is possible to assume that number A is divided completely into p_i, i.e. $\alpha_i = 0$, since otherwise we could examine the division of number $A' = A - \alpha_i$, which satisfies this condition. Let it be further

$$p_i = (\pi_1, \pi_2, \ldots, \pi_{i-1}, 0, p_i, p_i, \ldots, p_i).$$

Then

$$\frac{A}{p_i} = (\gamma_1, \gamma_2, \ldots, \gamma_{i-1}, \gamma_i, \gamma_{i+1}, \ldots, \gamma_n) =$$
$$= \left(\frac{\alpha_1}{\pi_1}, \frac{\alpha_2}{\pi_2}, \ldots, \frac{\alpha_{i-1}}{\pi_{i-1}}, \frac{0}{0}, \frac{\alpha_{i+1}}{p_i}, \ldots, \frac{\alpha_n}{p_i} \right).$$

Here all digits of quotient $A p_i$, except digit γ_i, are determined very simply - by the formal division of digit into appropriate digit p_i. Therefore the goal of obtaining the quotient A/p_i in this case is reduced to the disclosure/expansion of this uncertainty/indeterminancy. Let us consider the series/row of the methods of determining the digit γ_i.

Theorem 3.30. Let in the system with bases/bases p_1, p_2, ..., p_n and range $\mathscr{P}$ preset number $A = (\alpha_1, \alpha_2, ..., \alpha_n)$ with minimum trace S^*_A, that separates completely into one of the basis of system p_i so that the obtained quotient they are

$$\frac{A}{p_i} = (\gamma_1, \gamma_2, ..., \gamma_n).$$

Then as digit γ_i on basis/base p_i in the quotient must be taken this digit, that the minimum trace of quotient $S^*_{\frac{A}{p_i}}$ would be equal to

$$S^*_{\frac{A}{p_i}} = \gamma_n - \left[\frac{\alpha_n - S^*_A}{p_i} \right]. \qquad (3.112)$$

Proof. Since $S^*_{\frac{A}{p_i}}$ are the minimum trace of quotient, then occurs the relationship/ratio

$$\frac{\mathscr{P}}{p_n}\left(\gamma_n - S^*_{\frac{A}{p_i}}\right) \leqslant \frac{A}{p_i} < \left(\gamma_n - S^*_{\frac{A}{p_i}} + 1\right)\frac{\mathscr{P}}{p_n}. \quad (3.113)$$

Respectively for the initial number A we have

$$(\alpha_n - S^*_A)\frac{\mathscr{P}}{p_n} \leqslant A < (\alpha_n - S^*_A + 1)\frac{\mathscr{F}}{p_n}. \quad (3.114)$$

Dale latter/last inequality on p_i we will obtain

$$\frac{\alpha_n - S^*_A}{p_i}\frac{\mathscr{P}}{p_n} \leqslant \frac{A}{p_i} < \frac{\alpha_n - S^*_A + 1}{p_i}\frac{\mathscr{P}}{p_n}. \quad (3.115)$$

Page 148.

Taking into account that

$$\frac{\alpha_n - S_A^*}{p_i} \geqslant \left[\frac{\alpha_n - S_A^*}{p_i}\right]$$

and

$$\frac{\alpha_n - S_A^* + 1}{p_i} \leqslant \left[\frac{\alpha_n - S_A^*}{p_i}\right] + 1,$$

inequality (3.115) can be registered in the form

$$\left[\frac{\alpha_n - S_A^*}{p_i}\right]\frac{\mathcal{P}}{p_n} \leqslant \frac{A}{p_i} < \left\{\left[\frac{\alpha_n - S_A^*}{p_i}\right] + 1\right\}\frac{\mathcal{P}}{p_n}.$$

Comparing the obtained inequality with (3.113), we will obtain

$$\gamma_n - S_{\frac{A}{p_i}}^\bullet = \left[\frac{\alpha_n - S_A^*}{p_i}\right],$$

whence it follows (3.112).

Corollary. The proved theorem determines the following algorithm of the disclosure/expansion of uncertainty/indeterminancy in the case in question:

1. From S_A^*, α_n and p_i is computed value

$$\left[\frac{\alpha_n - S_A^*}{p_i}\right].$$

2. Are computed digits of formal quotient A/p_i, besides digit γ_i.

3. Is computed minimum trace of quotient

$$S_{\frac{A}{p_i}}^* = \gamma_n - \left[\frac{\alpha_n - S_A^*}{p_i} \right].$$

4. Is computed sum

$$Q = (S_{\gamma_1}^* + S_{\gamma_2}^* + \ldots + S_{\gamma_{i-1}}^* + S_{\gamma_{i+1}}^* + \ldots + S_{\gamma_{n-1}}^*)(\text{mod } p_n).$$

5. Is computed

$$(S_{\gamma_i}^*)_\Phi = (S_{\frac{A}{p_i}}^* - Q)(\text{mod } p_n)$$

and from $(S_{\gamma_i}^*)_\Phi$ is determined such digit γ_i, for which difference $S_{\gamma_i}^* - (S_{\gamma_i}^*)_\Phi$ is minimum.

Let us illustrate the method examined by an example. Let be preset the system of the bases/bases: $p_1 = 3$; $p_2 = 5$; $p_3 = 7$; $p_4 = 13$; $p_5 = 31$; with range $\mathscr{P} = 42315$.

The orthogonal bases of this system are equal to:

$$B_1 = 28\,210, \quad B_2 = 16\,926, \quad B_3 = 12\,090, \quad B_4 = 26\,040, \quad B_5 = 1365.$$

Page 149.

Example. To divide number $A = (1, 0, 0, 1, 25)$ with minimum trace $S_A^* = 23$ into basis/base $p_2 = 5 = (2, 0, 5, 5, 5)$.

In accordance with the algorithm given above, we produce the following operations:

1. We compute

$$\left[\frac{\alpha_n - S_A^*}{p_2}\right] = \left[\frac{25 - 23}{5}\right] = 0.$$

2. We compute digits of formal quotient

$$\left(\frac{A}{p_2}\right)_\psi = (2, \gamma_2, 0, 8, 5).$$

3. We compute minimum trace of quotient

$$S_{\frac{A}{p_2}}^* = 5 - 0 = 5.$$

4. We compute sum

$$Q = 21 - 3 = 24.$$

5. We compute

$$(S_{\gamma_2}^*)_\Phi = (5 - 24) \ (\bmod\ 31) = 12.$$

From the table of minimum pseudo-orthogonal numbers on basis/base $p_2 = 5$:

$$M_{12} = (0, 1, 0, 0, 19), \ M_{22} = (0, 2, 0, 0, 7), \ M_{32} = (0, 3, 0, 0, 25),$$
$$M_{42} = (0, 4, 0, 0, 13),$$

we find $S_{\gamma_2}^* = 13$. Hence $\gamma_2 = 4$. Thus, final quotient are $\frac{A}{p_2} = (2, 4, 0, 8, 5)$.

Although this method consists of the series/row of operation, enumerated of certain sequence however almost they all can be accomplished in parallel and therefore this method barely is dilated/extended in the time.

On the basis of theorem (3.30) it is possible to organize division and to the product of several bases/bases, performing in parallel division into each basis/base individually.

Let us consider as an example division into product $D=5\cdot7=35$.

Example. To divide number $A=(1, 0, 0, 1, 25)$, into $p_2 p_3 = 5\cdot7 = (2, 0, 5, 5, 5)$ $(1, 2, 0, 7, 7) = (2, 0, 0, 9, 4)$.

Division into the product can be carried out in parallel and simultaneously determined value $A/5$ and $A/7$, and then is determined $A/35$. The quotient $A/5$ was by us determined in previous with the measure, namely

$$\frac{A}{p_2} = \frac{A}{5} = (2, 4, 0, 8, 5).$$

Page 150.

Let us determine the quotient

$$\frac{A}{p_3} = \frac{A}{7}.$$

1. Let us compute

$$\left[\frac{a_n - S_A}{p_3}\right] = \left[\frac{25-23}{7}\right] = 0.$$

2. Let us compute digits of formal quotient

$$\left(\frac{A}{p_3}\right)_\Phi = (1, 0, \gamma_3, 2, 8).$$

3. Let us determine minimum trace of quotient

$$S^{\bullet}_{\frac{A}{p_3}} = 8 - 0 = 8.$$

4. Let us compute sum

$$Q = (11 + 24) \,(\text{mod} \, 31) = 4.$$

5. Let us determine $(S^{\bullet}_{\gamma_3})_\phi$:

$$(S^{\bullet}_{\gamma_3})_\phi = 8 - 4 = 4, \text{ откуда } \gamma_3 = 3.$$

Thus, we obtain

$$\frac{A}{p_3} = (1, 0, 3, 2, 8).$$

New quotient of the division of number A into the product of bases/bases $p_2 p_3$ can be determined on the basis of theorem 3.24 about the division into the product of numbers, namely:

$$\frac{A}{p_2 p_3} = \mu_1 \frac{A}{p_2} + \mu_2 \frac{A}{p_3},$$

where μ_1 and μ_2 - integers.

Here $\mu_1 = -2$, $\mu_2 = 3$, then

$$\frac{A}{p_2 p_3} = \frac{A}{35} = -(1, 3, 0, 3, 10) + (0, 0, 2, 6, 24) = (2, 2, 2, 3, 14) = 107.$$

Actually/really,

$$\frac{A}{p_2 p_3} = \frac{3745}{35} = 107.$$

§3.11. General case of division.

Let us consider now the division of number A into the arbitrary divider/denominator B. Here it would be possible to construct process, in the accuracy reproducing ordinary algorithm of positional division, realized by consecutive subtractions and shifts/shears.

Page 151.

However, it is considered by advisable to construct division in such a way that in it is possible the larger measure to use a specific character of operations in the residual classes. In this plan/layout as the elementary operation of division it is possible to take the division on any of the bases/bases whose execution was already described above.

Let us consider the following process. Let one of the basis of system $p_1 = 2$. Let us take 2 as the elementary divisor.

The 1st stage: is divided B to 2. We obtain B_1, divide B_1 by 2, obtain B_2 and so k of times where $B_k = 1$.

In parallel with this we divide A:2, obtain A_1, divide $A_1:2$, obtain A_2 and so to A_k. Number A_k is the first intermediate quotient.

The 2nd stage: is computed 1st discrepancy $A - BA_k$ C^1

The 3rd stage: it is computed
$$\frac{C^1}{2} = C_1^{(1)}; \quad \frac{C_1^{(1)}}{2} = C_2^{(1)}; \quad \ldots; \quad \frac{C_{k-1}^1}{2} \quad C_k^1$$

The 4th stage: is computed 2nd discrepancy $C^{(1)} - C_k^{(1)} \cdot B = C^{(2)}$.

These stages are repeated to those pores, thus far discrepancy is reduced to zero. Then the quotient

where
$$C = \frac{A}{B} = A_k - C_k^{(1)} + \ldots + C_k^{(l)},$$
$$C_k^{(l+1)} = 0.$$

Observation. Wherever is examined division into 2 it is intended either exact quotient, when dividend is multiple 2 or is near smaller to it.

This algorithm of division can be differently modified for the purpose of the acceleration cr its convergence. However, we will not stop during these modifications, but let us consider the development of this algorithm with the use/application of several bases/basis. The fact is that the use only of a one basis/base, equal to 2, requires a comparatively large number of divisions within the stage until the divided divider/denominator becomes equal to unity. Therefore it is expedient to use several bases/bases in order, on one hand, to decrease the capacity of operations within the stage, and on the other hand - to reduce the number of stages.

Let us select three bases/bases $p_1=2$, $p_2=3$, $p_3=5$. As it is
above, by the element/cell, which are determining character and
capacity of operations, is divider/denominator $B = (\beta_1, \beta_2, \ldots, \beta_n)$.

Page 152.

The content of stages in this case is such:

the 1st stage. Are computed the quotients

$$B_1 = \frac{B}{p_{i_1}}, \quad B_2 = \frac{B_1}{p_{i_2}}, \quad \ldots, \quad B_k = \frac{B_{k-1}}{p_{i_k}} = 1.$$

where $p_{i_1}, p_{i_2}, \ldots, p_{i_k}$ - any of the bases/bases 2, 3, 5.

The selection of basis/base, into which it is necessary to
perform division in each case, is determined as follows:

a) if $\beta_3=0$, 1 or 4, then division is performed on $p_3=5$, moreover
with $\beta_3=1$ divider/denominator B is reduced by 1, and with $\beta_3=4$
divider/denominator B increases by 1. But if $\beta_3=2$ or 3, then it is
examined digit on basis/base p_2:

b) if $\beta_2=0$, then division it is performed on $p_2=3$, if $\beta_2=1$ or 2
and $\beta_1=1$, then also is performed division into $p_2=3$, moreover with
$\beta_2=1$ divider/denominator is reduced by 1, and with $\beta_2=2$

divider/denominator increases by 1. With $\beta_2 = 1$ or 2, and $\beta_1 = 0$ the division is produced on $p_1 = 2$.

In parallel with this is produced division A into the same quotients into which was divided B, moreover rounding to the multiple must be produced in the same directions (i.e. by subtraction or by addition), that also during the division of divider/denominator. In this way is obtained first intermediate quotient A_k.

The 2nd stage. Is computed first discrepancy $C^{(1)} = A - BA_k$.

The 3rd stage. Is performed, as the first stage, but with dividend $C^{(1)}$.

In this case, if has the capability to memorize appropriate dividers/denominators $p_{i_1}, p_{i_2}, \ldots, p_{i_k}$ and the character of the rounding, carried out for obtaining the multiple during the division into these dividers/denominators, then there is no necessity to repeatedly produce division of B and content of stage it is reduced only to division $C^{(1)}$, to obtaining $C_1^{(1)}, C_2^{(1)}, \ldots, C_k^{(1)}$.

If $C_k^{(1)} = 0$, then division on this is finished, but if $C_k^{(1)} \neq 0$, then is computed discrepancy $C^{(2)} = C^{(1)} - BC_k^{(1)}$ and with it enter analogously.

So are repeated the stages of the calculations of intermediate quotients and discrepancies up to obtaining of zero intermediate quotient $C_k^{(l)} = 0.$

Full/total/complete quotient

$$C = \frac{A}{B} = A_k + C_k^{(1)} + C_k^{(2)} + \ldots + C_k^{(l-1)}.$$

Page 153.

Example. Is preset system with the bases/bases: $p_1=2$, $p_2=3$, $p_3=5$, $p_4=11$, $p_5=13$, with range $\mathscr{P} = 4290$.

To divide number A=(1, 0, 1, 3, 1) into number B=(0, 1, 3, 8, 1).

The 1st stage: they are computed:

$$B_1 = \frac{(0, 1, 3, 8, 1)}{2} = (1, 2, 4, 4, 7),$$

$$B_2 = \frac{(1, 2, 4, 4, 7)}{5} \approx \frac{(0, 0, 0, 5, 8)}{5} = (0, 0, 2, 1, 12);$$

$$B_3 = \frac{(0, 0, 2, 1, 12)}{3} = (0, 1, 4, 4, 4),$$

$$B_4 = \frac{(0, 1, 4, 4, 4)}{5} \approx \frac{(1, 2, 0, 5, 5)}{5} \quad (1, 1, 1, 1, 1).$$

Parallel operations with the dividend:

$$A_1 = \frac{(1, 0, 1, 3, 1)}{2} \approx \frac{(0, 2, 0, 2, 0)}{2} = (0, 1, 0, 1, 0),$$

$$A_2 = \frac{(0, 1, 0, 1, 0)}{5} = (0, 2, 1, 9, 0),$$

$$A_3 = \frac{(0,\ 2,\ 1,\ 9,\ 0)}{3} \approx \frac{(1,\ 0,\ 2,\ 10,\ 1)}{3} = (1,\ 1,\ 4,\ 7,\ 9).$$

$$A_4 = \frac{(1,\ 1,\ 4,\ 7,\ 9)}{5} \approx \frac{(0,\ 2,\ 0,\ 8,\ 10)}{5} = (0,\ 1,\ 3,\ 6,\ 2).$$

First intermediate quotient $A_4 = (0,\ 1,\ 3,\ 6,\ 2)$.

The 2nd stage: is computed the first discrepancy

$$C^{(1)} = (1,\ 0,\ 1,\ 3,\ 1) - (0,\ 1,\ 3,\ 8,\ 1) \cdot (0,\ 1,\ 3,\ 6,\ 2) = (1,\ 2,\ 2,\ 10,\ 12).$$

The 3rd stage: the repetition of the 1st stage for $C^{(1)} = (1,\ 2,\ 2,\ 10,\ 12)$

$$C_1^{(1)} = \frac{(1,\ 2,\ 2,\ 10,\ 12)}{2} \approx \frac{(0,\ 1,\ 1,\ 9,\ 11)}{2} = (0,\ 2,\ 3,\ 10,\ 12).$$

$$C_2^{(1)} = \frac{(0,\ 2,\ 3,\ 10,\ 12)}{5} \approx \frac{(0,\ 1,\ 0,\ 1,\ 1)}{5} = (0,\ 2,\ 1,\ 9,\ 8).$$

$$C_3^{(1)} = \frac{(0,\ 2,\ 1,\ 9,\ 8)}{3} \approx \frac{(1,\ 0,\ 2,\ 10,\ 9)}{3} = (1,\ 2,\ 4,\ 7,\ 3).$$

$$C_4^{(1)} = \frac{(1,\ 2,\ 4,\ 7,\ 3)}{5} \approx \frac{(0,\ 0,\ 0,\ 8,\ 4)}{5} = (0,\ 0,\ 1,\ 6,\ 6).$$

Second intermediate quotient $C_4^{(1)} = (0,\ 0,\ 1,\ 6,\ 6)$.

The 4th stage: is computed the second discrepancy

$$C^{(2)} = (1,\ 2,\ 2,\ 10,\ 12) - (0,\ 1,\ 3,\ 8,\ 1) \cdot (0,\ 0,\ 1,\ 6,\ 6) = (1,\ 2,\ 4,\ 6,\ 6).$$

Page 154.

The 5th stage: the repetition of the 1st stage for $C^{(2)} = (1,\ 2,\ 4,\ 6,\ 6)$

$$C_1^{(2)} = \frac{(1, 2, 4, 6, 6)}{2} \approx \frac{(0, 1, 3, 5, 5)}{2} = (0, 2, 4, 8, 9),$$

$$C_2^{(2)} = \frac{(0, 2, 4, 8, 9)}{5} \approx \frac{(1, 0, 0, 9, 10)}{5} = (1, 0, 0, 4, 2),$$

$$C_3^{(2)} = \frac{(1, 0, 0, 4, 2)}{3} = (1, 2, 0, 5, 5),$$

$$C_4^{(2)} = \frac{(1, 2, 0, 5, 5)}{5} = (1, 1, 1, 1, 1).$$

On this the division can be finished, since the following discrepancy compulsorily will already be zero. Let us compose the quotient

$$\frac{(1, 0, 1, 3, 1)}{(0, 1, 3, 8, 1)} = (0, 1, 3, 6, 2) - (0, 0, 1, 6, 6) -$$
$$+ (1, 1, 1, 1, 1) = (1, 2, 0, 2, 9).$$

Let us do some observations to the described algorithm:

1. The selection of bases/bases $p_{i_1}, p_{i_2}, \cdots, p_{i_k}$ for the concrete/specific/actual system of bases/bases can be realized differently, but it is compulsorily linten with the special features/peculiarities of these bases/bases.

2. Set of conditions, on which in each individual case in first stage is realized selection of concrete/specific/actual basis/base from set $p_{i_1}, p_{i_2}, \cdots, p_{i_k}$ can be differently formulated. In particular, can be formulated the conditions, which one way or another considered also the digits of dividend. Of this type the more refined conditions could to a considerable extent decrease a quantity of iterations (stages) and a capacity of operations in each stage. In this case it

can seem that the playing the leading role divider/denominator could in different stages in different ways determine set $p_{i_1}, p_{i_2}, \ldots, p_{i_k}$.

Determination of analytically of the necessary set of elementary divisors, set of conditions for their selection and evaluation of convergence is difficult and hardly appropriate. The basic method of the study of these questions is the method of statistical modeling with the help of which it is shown that an average number of iterations which should be led for obtaining the quotient in the sufficiently broad band (order 10^{10}), does not exceed three.

Chapter 4.

SELF-CORRECTING CODES IN THE SYSTEM OF RESIDUAL CLASSES.

§4.1. On the codes with detection and correction of errors.

The multiple research, carried out in the latter/last decade,
convincingly justified the possibility of the construction of such
information-carrying systems in which due to the special coding can
be created the immunity against the most diverse distortions of
intelligence signals. Completely clearly was formed the point of
view, that the fight for the high reliability of the transmission of
information, i.e., for the authenticity of information retrieval at
receiving end of the transmission line, must be conducted not so much
by the perfection of the technical transmission media of the
information where any possible increase in the reliability is
achieved by high price and now and then requires the development of
complicated protective measures, as by use/application of such
methods of the coding of information which would be stable with
respect to the possible random distortions of information,
understanding by this the ability by corresponding processing of the
information accepted to exclude the introduced into it

disturbances/perturbations, to clean it from the errors and to
achieve complete agreement what was transmitted from the transmitting
end of the line.

Page 156.

While the increase in reliability of the transmission of
information by technical equipment, even if we are not considered the
economic side of a question, is limited by the level of the
development of technology of communications and any considerable
achievements in this region require the new technical solutions,
use/application for the same target of special code systems contains
no fundamental limitations. Moreover, when selecting
adequate/approaching code, which possesses the necessary corrective
ability, it is possible to noticeably reduce requirements for the
reliability of very lines of transmission of information, to make
them simpler and cheaper.

For the computational means the use/application of methods of
special coding is dictated by most vital need. Indeed any computer is
itself the transmission system and information processing. In the
computer occurs constantly the circulation of information. Although
in the machine there are no long transmission lines, but along the
available in it relatively short lines information circulates with

the enormous velocity also in large quantities. If we take some
arbitrary unit, for example passage as one bit of one centimeter of
path, then in these arbitrary units the work of one computer of
average efficiency in the fixed/recorded time interval on the
transmission of information will be commensurated with the work in
the same interval of the series/row of the large state transmission
lines.

Therefore even from the point of view only of the transmission
of information during the development of computational means appears
the important task of guaranteeing the authenticity of entire
colossal information flow. But indeed in the computer, furthermore,
it must be provided even and the authenticity of arithmetic and
logical information processing. In practice without the
use/application of methods of special coding the guarantee of
authenticity in the computer is achieved by double error for the
detection of correctness or inaccuracy of the results of the solution
of problems and by triple error in the case of the discovered
disagreement for the selection of correct result according to
coinciding data. This way of guaranteeing the authenticity reduces
the actual productivity of machine at least doubly. It is hence clear
that the guarantee of authenticity with any methods, different from
the repeated errors indicated, directly and is directly connected
with an increase in the productivity of computers.

Page 157.

For each spacial code of which it is required so that it would possess the capability for detection and correction of error, is characteristic the presence of two groups of digits - informational and control room. Into informational group enter the digits, which compose the numerical value of the coded quantity, while into the control group - digits, additionally introduced for purposes of detection and correction of possible transmitter distortions. These further digits are surplus from the point of view of the numerical value of quantity and lengthen the total length of the code, that it goes without saying somewhat reduces as the final result the channel capacity during serial transfer and increases a quantity of channels during the parallel transmission. However, these circumstances must be redeemed by those possibilities which obtain surplus digits for the detection and corrections of errors.

Let us designate through J_A *and* K_A the respectively informational and the control room of the part of code A. Control part K_A is the function of the informational part: $K_A = F(J_A)$

The form of the function F and, therefore, the character of the

introduced into the code check digits they are determined by the
adopted system of coding.

Let in this transmission system and information processing be is
accepted the n-bit binary positional representation of numerical
values, i.e., all operations are produced on numbers (being
distracted from the scales) in the range $[0,2^n)$. After introducing into
the representation still m of control binary digits, we will use with
numbers in the range $[0,2^{n+m})$. However, this expansion of overall range
does not in any way increase the range in which can be represented
and be treated numerical data, since the introduced digits do not
carry informational functions. Let entire code A be written/recorded
by the set of binary digits ε_j

$$A = \{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n, \widetilde{\varepsilon}_{n+1}, \widetilde{\varepsilon}_{n+2}, \ldots, \widetilde{\varepsilon}_{n+m}\}.$$

Here

$$J_A = \{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n\}; \quad K_A = \{\widetilde{\varepsilon}_{n+1}, \widetilde{\varepsilon}_{n+2}, \ldots, \widetilde{\varepsilon}_{n+m}\}.$$

The basic special feature/peculiarity of all known up to now special
positional codes is the disparity of informational and control room
of the parts of the code relative to arithmetic operations.

Page 158.

Let J_A, K_A and J_B, K_B be informational and with respect the control
parts of the codes of numbers A and B, and let on J_A and J_B be

performed certain arithmetic operation $f(J_A, J_B)$. Both parts of the code would be equal, if operation f was accomplished above the full/total/complete code, i.e., would be computed value

$$C = f(A, B), \qquad (4.1)$$

moreover $$J_c = f(J_a, J_b).$$

Then, after computing $K_c^1 = F(J_c)$ and after comparing it with K_c — by actual control part of code C, it is possible to control the correctness of the execution of operation f. Even more the equitableness of both parts of the code would be expressed, if besides (4.1) had place also equality

$$K_c = f(K_A, K_B).$$

Meanwhile in the known positional codes operation f is produced not above the full/total/complete code of numbers A and B, but above J_A and J_B, is obtained $C^1 = f(J_A, J_B)$, while K_c is computed as $F(C^1)$, after which is comprised the full/total/complete code C, for which $J_c = C^1$. Here K_A and K_B in the arithmetic operation do not participate, that it gives no possibility on the control parts of the components of arithmetic operation to compose the control part of the result, i.e., is excluded the possibility of the check of the correctness of the execution of arithmetic operations.

Specifically, this property of the special positional codes (their nonarithmeticity) impedes their use/application in the

computers, since the introduced check bits do not make it possible to
monitor the result of arithmetic operation, while this check for the
computer not is less important than the control of the transmission
of information.

At present in connection with the development of machine
arithmetic in the system of residual classes arose the possibility of
the construction of the nonpositional codes, which discover and which
correct errors, and at the same time of the completely arithmetic
codes where informational and control room of part is completely
equal relative to any operation.

Page 159.

Let us consider system with bases/bases p_1, p_2, ... p_n and range
$\mathcal{P} = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Subsequently range $\mathcal{P}$ we will call the operating range
of system. Let us introduce basis/base p_{n+1} mutually simple with any
of the bases/bases accepted we will represent numbers in the system
from n+1 bases/bases. This means that we will transmit numbers and
perform the operations on the numbers, which lie in the range $[0, \mathcal{P})$,
in the broader band $[0, P]$, where $P = \mathcal{P} p_{n+1}$.

Subsequently range P we will call the full/total/complete range
of system with one control basis/base.

Since we agreed, that all numbers, with which it uses computer, they must lie/rest in the range $[0, \mathscr{P})$, then it is obvious that if as a result of any operation or during the transmission of a number it turned out that is obtained number A, larger $\mathscr{P}$, then, this means, while the carrying out of operation it was permitted error.

We will subsequently of the number smaller than $\mathscr{P}$, call correct, and large $\mathscr{P}$ — incorrect.

Theorem 4.1. Let bases/bases p_1, p_2, ..., p_n, p_{n+1} the systems of residual classes satisfy the condition
$$p_i < p_{n+1},$$
$$i = 1, 2, \ldots, n,$$
and let $A = (\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n, \alpha_{n+1})$ — correct number.

Then number $\tilde{A} = (\alpha_1, \alpha_2, \ldots, \alpha_i \neq \alpha_i, \ldots, \alpha_n, \alpha_{n+1})$, where $i = 1, 2, \ldots, n, n+1$ is incorrect.

Proof. The correctness of number A regarding/means that the definition
$$A < \frac{P}{p_{n+1}},$$
however, since
$$\frac{P}{p_i} \geqslant \frac{P}{p_{n+1}},$$
$$i = 1, 2, \ldots, n+1,$$

then all the more
~~that as of old~~

$$A < \frac{P}{p_i}.$$

As soon as $\tilde{\alpha}_i \neq \alpha_i$, number $\tilde{A}$ cannot be located in interval $\left[0, \frac{P}{p_i}\right)$.

$$\tilde{A} > \frac{P}{p_i}.$$

but then has the place

$$\tilde{A} > \frac{P}{p_{n+1}},$$

i.e. $\tilde{A}$ is an incorrect number.

Page 160.

Thus established/installed the very important fact, which is determining the possibility of the construction of the discovering and corrective codes in the system of residual classes, namely: any distortion of digit of any one digit converts this number into the incorrect and thereby it permits to discover the presence of distortion. Moreover, there is only a only one value of this digit, which can convert an incorrect number into the correct.

As we see, theorem is proved on the assumption that the additionally introduced basis/base is greater than any of the basis of system. This determines the rule of the selection of control basis/base p_{n+1} — it must be large of any basis of system.

It is necessary to note that by the same path can be proved

somewhat more strong fact. among the foundations for eating such

small bases/bases $p_{j_1}, p_{j_2}, \ldots, p_{j_k}$, that

$$\prod_{t=1}^{k} p_{j_t} = \overline{P} < p_{n+1}.$$

Then any distortions in the digits on several ones or even on all

these bases/bases convert a correct number into the incorrect, and

therefore in all these cases the presence of distortions can be

established/installed.

For the proof it is possible to consider the product of these

bases/bases $\overline{P}$ as one basis/base, and since is observed condition

$\overline{P} < p_{n+1}$, then there will be correctly and the assertion of latter/last

theorem. Any distortion of digit on basis/base $\overline{P}$ can affect digits on

several ones or even on all entering $\overline{P}$ bases/bases. Thus, in order to

discover presence or absence of the error in number A, it is

necessary to compare it with range $\mathscr{P}$. In this case, if it proved to

be $A \geqslant \mathscr{P}$,   occurred the error at least in one digit. But if $A < \mathscr{P}$,

then either there is no error or it carries more complicated

character.

Page 161.

Let us consider some examples. Let us select the system of

bases/bases $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, for which the range of correct

values (operating range) $\mathscr{P} = 2 \cdot 3 \cdot 5 \cdot 7 = 210$. Let us introduce the control

basis/base $p_5=11$. Then full/total/complete range is defined as:
$p=210 \cdot 11 = 2310$.

Let us compute the orthogonal bases of the system:

$$B_1 = (1, 0, 0, 0, 0) = 1155; \quad B_2 = (0, 1, 0, 0, 0) = 1540;$$
$$B_3 = (0, 0, 1, 0, 0) = 1386; \quad B_4 = (0, 0, 0, 1, 0) = 330;$$
$$B_5 = (0, 0, 0, 0, 1) = 210.$$

Example. Is transmitted number $A=(1, 2, 2, 3, 6)=17$. Instead of it proved to be taken number $\tilde{A} = (1, 2, 2, 5, 6)$. For the detection of error we compute value $\tilde{A}$

$$\tilde{A} = 1 \cdot 1155 + 2 \cdot 1540 + 2 \cdot 1386 + 5 \cdot 330 + 6 \cdot 210 - r2310 =$$
$$= 9917 - 9240 = 677 > 210.$$

Since is accepted number $\tilde{A}$ of more than 210, it is incorrect. Thereby is discovered the presence of error during the transmission of a number.

Example. Is transmitted the same number 17. It is accepted $\tilde{A} = (1, 2, 2, 3, 0)$ - is distorted digit on the control basis/base. We compute value $\tilde{A}$:

$$\tilde{A} = 1 \cdot 1155 + 2 \cdot 1540 + 2 \cdot 1386 + 3 \cdot 330 + 0 \cdot 210 - r2310 =$$
$$= 7997 - 6930 = 1067 > 210.$$

Thus $\tilde{A} > 210$, which indicates the presence of error.

Example. Instead of number $A=17$, is accepted number $\tilde{A}=(0, 2, 3, 3, 6)$. Here to distortion underwent digits on bases/bases 2 and 5. Since $\overline{p} = 2 \cdot 5 = 10 < p_5$, this distortion must be discovered.

Actually/really:

$$\tilde{A} = 0 \cdot 1155 + 2 \cdot 1540 + 3 \cdot 1386 + 3 \cdot 330 - 6 \cdot 210 - r2310 =$$
$$= 9488 - 9240 = 248 > 210.$$

Thus, $\tilde{A}$ — incorrect number.

Let us give now the example when on the bases/bases whose product exceeds 11, can occur the undetectable distortions.

Example. Instead of number A=17 it is accepted $\widetilde{A}$=(1, 2, 2, 0, 0).

$$\tilde{A} = 1 \cdot 1155 + 2 \cdot 1540 + 2 \cdot 1386 + 0 \cdot 330 + 0 \cdot 210 - r2310 =$$
$$= 7007 - 6930 = 77 < 210.$$

Thus, $\tilde{A}$ was obtained as a correct number. The fact of distortion in two digits was not discovered.

§4.2. Corrective properties of the special codes.

For the research of the corrective possibilities of the code examined important value has the following theorem.

Page 162.

Theorem 4.2. Let bases/bases p_1, p_2, ..., p_n, p_{n+1} the systems of residual classes satisfy the condition

$$p_i < p_{n+1},$$
$$i = 1, 2, ..., n.$$

and let A=(α_1, α_2, ..., α_i, ..., α_n, α_{n+1}) — correct number. Then value A

is not changed, if we will represent it in the system of bases/bases
from which is withdrawn basis/base p_i (i.e. if we in representation A
delete digit a_i).

Proof. Inequality $A < \frac{P}{p_i}$ to the absolute inequality

$$A < p_1 p_2, \ldots, p_{i-1} p_{i+1}, \ldots, p_{n+1},$$

and, therefore, number A can be in a only manner represented by its
remainders/residues on these bases/bases, that also is claimed in the
theorem.

Determination. Let us name number A_i, obtained from A by the
crossing out of digit a_i, the projection of number A on basis/base p_i.

Determination. The system of bases/bases p_1, p_2, ..., p_n, p_{n+1},
that satisfies the condition

$$p_1 < p_2 < \ldots < p_n < p_{n+1},$$

we will call the regulated system of bases/bases. Let us formulate
the following theorem.

Theorem 4.3. If in the regulated system of bases/bases is preset
the correct number $A = (a_1, a_2, \ldots, a_i, \ldots, a_n, a_{n+1})$, then the projections
of this number in all bases/bases coincide, i.e.,

$$A_1 = A_2 = \ldots = A_i = \ldots = A_{n+1} < \frac{P}{p_{n+1}}.$$

Proof. For a correct number under the condition the theorems

take the place of the inequality

$$A < \frac{P}{p_{n+1}} < \frac{P}{p_n} < \ldots < \frac{P}{p_i} < \ldots < \frac{P}{p_1},$$

and in accordance with the previous theorem value A will preserve its projection on each of the bases/bases.

Theorem 4.4 (reverse). If in regulated system of the basis of the projection of number $A = (\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n, \alpha_{n+1})$ in all bases coincide, then number A is correct.

Page 163.

Proof. Let us lead proof by contradiction. Let A an incorrect number and in it be inaccurate digit α_i. Let us replace it by correct $\tilde{\alpha}_i$. We will obtain the number

$$\tilde{A} = (\alpha_1, \alpha_2, \ldots, \tilde{\alpha}_i, \ldots, \alpha_{n+1}).$$

which, by hypothesis, is correct. Consequently, its projections are equal to each other

$$\tilde{A}_1 = \tilde{A}_2 = \ldots = \tilde{A}_i = \ldots = \tilde{A}_{n+1}.$$

But in view of the fact that $\tilde{A}_i$ identically coincides with A as those composed of one and the same digits, then must be

$$A_1 = \tilde{A}_1 = A_2 = \tilde{A}_2 = \ldots = A_{n+1} = \tilde{A}_{n+1}.$$

which is impossible, since projections A_j with $j \neq i$ differ from A_j in terms of digit in basis/base p_i and therefore A_i cannot coincide with A_j. Thus, is rejected assumption about the inaccuracy of number A.

In a number of cases in the values of projections it is possible
to draw conclusions about the correctness of single digits. Thus, for
instance, occurs the following theorem.

Theorem 4.5. If in the regulated system of bases/bases
projection A_i of number $A = (\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n, \alpha_{n+1})$ on basis/base
p_i satisfy the condition

$$A_i > \frac{P}{p_{n+1}}, \qquad (4.2)$$

then digit α_i is correct, if is possible only single (in the digit of
any one basis/base) error.

Proof. Let us assume that digit α_i is erroneous. Since the error
can be only one, remaining digits correct. Consequently, projection
A_i as composed of the correct digits must be a correct number, and
this contradicts theorem condition. Thereby is proved the
groundlessness of assumption about the inaccuracy of digit α_i.

Corollary. If (4.2) occurs for all i=1, 2, ..., n, then is
erroneous digit α_{n+1}.

Proof. Let us first of all note that projection A_{n+1} is always a
correct number and, therefore, for it (4.2) cannot have the places.

Under conditions of corollary is set consecutively/serially the correctness of digits α_1, α_2, ..., α_n, and since the error nevertheless is, it unavoidably is contained in digit α_{n-1}.

Page 164.

Somewhat another character carries the following theorem, which makes it possible to range of the cases the correctness of one or the other group of digits.

Theorem 4.6. Let in the regulated system of bases/bases the number

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1})$$

satisfy the condition $\dfrac{P}{p_{n-1}} < A < \dfrac{P}{p_j}$,

then digits α_1, α_2, ..., α_j on bases/bases p_1, p_2, ..., p_j correct, if is possible only isolated error.

Proof. Let us first of all set the correctness of digit α_j under theorem conditions. Let us assume that α_j is incorrect, and correct is digit $\tilde{\alpha}_j$. Let us designate correct number through $\widetilde{A}$. Then it is possible to write, on the basis of the disintegration of numbers A and $\widetilde{A}$ in terms of the orthogonal bases, that

$$\tilde{A} = A + (\tilde{\alpha}_j - \alpha_j)\, B_j = A + (\tilde{\alpha}_j - \alpha_j)\, m_j \frac{P}{p_j}.$$

A maximally possible value for value $(\tilde{\alpha}_j - \alpha_j) m_j \frac{P}{p_j}$ (throwing/rejecting the wholes P) exists $\frac{p_j - 1}{p_j} P$.

$$\tilde{A} < \frac{P}{p_j} + \frac{p_j - 1}{p_j} P = P. \qquad (4.3)$$

Number $\tilde{A}$ could be correct, i.e., smaller than $\frac{P}{p_{n+1}}$, only in such a case, when from the introduction of correction in the form of addition $(\tilde{\alpha}_j - \alpha_j) B_j$ it exceeded P. Meanwhile inequality (4.3) shows that by any possible correction of digit α_j this cannot be achieved. Therefore, digit α_j correct. Hence automatically follows the correctness of all digits in bases/bases less p_j, since inequality $A < \frac{P}{p_j}$ indicates the inequalities

$$A < \frac{P}{p_{j-1}} < \frac{P}{p_{j-2}} < \ldots < \frac{P}{p_1}.$$

but from each of these inequalities individually follows the correctness of the corresponding digit.

Page 165.

Obvious corollary of this is the fact that with j=n erroneous is digit α_{n+1}.

Let us give some illustrating established facts examples in the system of the bases/bases: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$.

Example. Is transmitted number A=(1, 2, 2, 3, 6)=17, it is accepted $\tilde{A}$=(1, 2, 2, 3, 7). For the detection of error let us compute

value $\widetilde{A}$:

$$\widetilde{A} = 1 \cdot 1155 + 2 \cdot 1540 + 2 \cdot 1386 - 3 \cdot 330 - 7 \cdot 210 - r2310 =$$
$$= 9467 - 9240 = 227.$$

Inequality 227>210 it establishes that $\widetilde{A}$ is incorrect.

Let us compute $\dfrac{P}{p_j}$:

$$\frac{P}{p_1} = 1155, \quad \frac{P}{p_2} = 770, \quad \frac{P}{p_3} = 462, \quad \frac{P}{p_4} = 330.$$

Comparing these values with $\widetilde{A}$, we obtain, that $\widetilde{A} < P/p_4$, therefore, erroneous is digit 7 on basis/base 11.

Example. Instead of number A = (1, 2, 2, 3, 6) it is accepted $\widetilde{A}$ = (1, 2, 2, 3, 4). We compute value $\widetilde{A}$

$$\widetilde{A} = 1 \cdot 1155 + 2 \cdot 1540 + 2 \cdot 1386 - 3 \cdot 330 - 4 \cdot 210 - r2310 =$$
$$= 8837 - 6930 = 1907.$$

Will compute the projections of number $\widetilde{A}$.

Projection on the first basis/base $\widetilde{A}_1$ = (2, 2, 3, 4).

Orthogonal bases in this case have the following values:

$$B_1^{(1)} = 385, \quad B_2^{(1)} = 231, \quad B_4^{(1)} = 330, \quad B_5^{(1)} = 210.$$
$$P_1 = 3 \cdot 5 \cdot 7 \cdot 11 = 1155;$$
$$\widetilde{A}_1 = 2 \cdot 385 + 2 \cdot 231 + 3 \cdot 330 + 4 \cdot 210 - r1155 = 752 > 210.$$

Projection on the second basis/base $\widetilde{A}_2$ = (1, 2, 3, 4).

In this case orthogonal bases are equal to:

$$B_1^{(2)} = 385, \quad B_3^{(2)} = 616, \quad B_4^{(2)} = 330, \quad B_5^{(2)} = 210.$$
$$P_2 = 2 \cdot 5 \cdot 7 \cdot 11 = 770$$
$$\widetilde{A}_2 = 1 \cdot 385 + 2 \cdot 616 + 3 \cdot 330 + 4 \cdot 210 - r770 = 367 > 21.$$

Projection on the third basis/base $\widetilde{A}_3 = (1, 2, 3, 4)$.

Orthogonal bases have the following values:

$$B_1^{(3)} = 231, \quad B_2^{(3)} = 154, \quad B_3^{(3)} = 330, \quad B_5^{(3)} = 210.$$
$$P_3 = 2 \cdot 3 \cdot 7 \cdot 11 = 462.$$
$$\widetilde{A}_3 = 1 \cdot 231 + 2 \cdot 154 + 3 \cdot 330 + 4 \cdot 210 - r462 = 59 < 210.$$

Page 166.

Projection on the fourth basis/base $\widetilde{A}_4 = (1, 2, 2, 4)$.

Orthogonal bases for these bases/bases are such:

$$B_1^{(4)} = 165, \quad B_2^{(4)} = 220, \quad B_3^{(4)} = 66, \quad B_5^{(4)} = 210.$$
$$P_4 = 2 \cdot 3 \cdot 5 \cdot 11 = 330.$$
$$\widetilde{A}_4 = 1 \cdot 165 + 2 \cdot 220 + 2 \cdot 66 + 4 \cdot 210 - r330 = 257 > 210.$$

Projection on the control basis/base $\widetilde{A}_5 = (1, 2, 2, 3)$.

We compute the orthogonal bases:

$$B_1^{(5)} = 105, \quad B_2^{(5)} = 70, \quad B_3^{(5)} = 126, \quad B_4^{(5)} = 120.$$
$$P_5 = 2 \cdot 3 \cdot 5 \cdot 7 = 210.$$
$$\widetilde{A}_5 = 1 \cdot 105 + 2 \cdot 70 + 2 \cdot 126 + 3 \cdot 120 - r210 = 17 < 210.$$

Thus, among five projections of the number $\widetilde{A}_1, \widetilde{A}_2$ and $\widetilde{A}_4$ accepted they exceed 210, and $\widetilde{A}_3$ and $\widetilde{A}_5$ is less than 210. Consequently, digits on bases/bases $p_1 = 2$, $p_2 = 3$, $p_4 = 7$ are correct. Erroneous can be digit on basis/base $p_3 = 5$, or on basis/base $p_5 = 11$.

The given above theorems made it possible under the appropriate

conditions to sat, which of the digits was erroneous. Then the
correction of erroneous digit is realized very simply. Let in the
number $\widetilde{A}$ accepted be erroneous digit $\widetilde{a}_i$. Designating the correct digit
through a_i, let us write the inequality

$$A = \widetilde{A} + (a_i - \widetilde{a}_i) B_i - kP < \frac{P}{p_{n+1}},$$

whence

$$a_i < \widetilde{a}_i + \frac{p_i(1+kp_{n+1})}{p_{n+1}m_i} - \frac{\widetilde{A}}{B_i}$$

or

$$a_i = \widetilde{a}_i + \left[\frac{p_i(1+kp_{n+1})}{p_{n+1}m_i} - \frac{\widetilde{A}}{B_i} \right]. \qquad (4.4)$$

According to formula (4.4) it is possible to compute the correct
value of digit on basis/base p_i, as soon as established/installed,
that the error occurs precisely in this digit.

Let us use this formula for the correction of erroneous digit in
examples examined above. Let us find correct digit. In the first
example is accepted number $\widehat{A}=(1, 2, 2, 3, 7)$ with the error on the
control basis/base. Let us determine true value of a_5

$$a_5 = 7 - \left[\frac{11(1+11)}{11} - \frac{227}{210} \right] = 6.$$

In the second example let us find the true value of erroneous digit
from the control basis/base

$$a_5 = 4 + \left[\frac{11(1+11)}{11} - \frac{1907}{210} \right] = 6.$$

Page 167.

§4.3. Codes with two control bases/bases.

We saw that the introduction only one control basis/base does not make it possible to in general localize erroneous digit. Let us consider now, what discovering and corrective possibilities possess the codes in the presence of two control bases/bases.

Thus, in addition to system examined earlier of the bases/bases

$$p_1, \; p_2, \; \ldots, \; p_n, \; p_{n+1}$$

we supplement basis/base $p_{n+2} > p_{n-1}$ and we will represent the numbers, which lie at operating range $[0, \mathscr{P})$, at the system, which has range $[0, P)$, where

$$P = p_{n+1} p_{n+2} \mathscr{P}.$$

Subsequently range P we will call the full/total/complete range of system with two control bases/bases. Correct we will consider, as earlier, the numbers, which lie in the range $[0, \mathscr{P})$.

Theorem 4.7. If is preset the system of bases/bases $p_1, \; p_2, \; \ldots,$ $p_n, \; p_{n+1}, \; p_{n+2}$ and if ρ from these bases/bases

$$p_{j_1}, \; p_{j_2}, \; \ldots, \; p_{j_\rho} \qquad\qquad (4.5)$$

are such, that is satisfied the condition

$$\prod_{k=1}^{\rho} p_{j_k} = \overline{p_j} < p_{n+1} p_{n+2} = \tilde{p}_{n+1}.$$

the number $\widetilde{\lambda}$, in which are erroneous the digits on all bases/bases (4.5) or on the part of them, it is incorrect.

Proof. If we consider $\bar{p}_j$ as one basis of system, and $\tilde{p}_{n-1}$ as one control basis/base, then is observed condition $\bar{p}_j < \tilde{p}_{n+1}$ and number, in which is erroneous the digit on basis/base $\bar{p}_j$, it is incorrect. However, the error in the digit on basis/base $\bar{p}_j$ can affect digits on all bases/bases $p_{j_1}, p_{j_2}, \ldots, p_{j_0}$ or on the part of them. By this theorem is proved.

Page 168.

Since each of the control bases/bases is chosen large any of the working bases/bases, then, whatever two of the basis of system p_i and p_j, including control rooms, will always take the place

$$p_i p_j \leqslant p_{n+1} p_{n+2}, \qquad (4.6)$$

for any i, j=1, 2, ..., n, n+1, n+2.

Consequently, a number with the double error, i.e., by the error in the digits of any two bases/bases, will be always incorrect and thereby the presence of error it can be established/installed.

Let us consider the examples, which illustrate the detection of the error in the system with two control bases/bases. Let us take the system of bases/bases $p_1=2$, $p_2=3$, $p_3=5$, $p_4=7$, $p_5=11$, $p_6=13$.

Bases/bases p_5 and p_6 we will consider control rooms. The operating range of system will be defined as $\mathscr{P} = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, and full/total/complete range as $P = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$.

Let us compute the orthogonal bases of this system:

$$B_1 = 15015, \quad B_2 = 20020, \quad B_3 = 6006, \quad B_4 = 25740,$$
$$B_5 = 16380, \quad B_6 = 6930.$$

Example. Is transmitted number $A = (1, 2, 2, 3, 6, 4) = 17$. Is accepted instead of it number $\widetilde{A} = (1, 0, 3, 5, 6, 4)$. We compute value $\widetilde{A}$:

$$\widetilde{A} = 1 \cdot 15\,015 + 2 \cdot 20\,020 + 3 \cdot 6006 + 5 \cdot 25\,740 + 6 \cdot 16\,380 + 4 \cdot 6930 -$$
$$- r30\,030 = 287\,733 - 270\,270 = 17\,463.$$

Thus, $\widetilde{A} > 210$. Inaccuracy $\widetilde{A}$ is discovered, although the error affected digits of three bases/bases: 3, 5, 7.

Example. Instead of $A = 17$ it is accepted $\widetilde{A} = (1, 2, 2, 3, 9, 7)$:

$$\widetilde{A} = 1 \cdot 15\,015 + 2 \cdot 20\,020 + 2 \cdot 6006 + 3 \cdot 25\,740 + 9 \cdot 16\,380 + 7 \cdot 6930 -$$
$$- r30\,030 = 340\,217 - 330\,330 = 9887.$$

Here error affects both control bases/bases, the presence of error is established/installed in view of $\widetilde{A} > 210$.

Let us now move on for the examination of the corrective possibilities of the adopted system.

Determination. Let us name number A_{ij}, obtained from A by the omission of digits on bases/bases p_i and p_j, by the projection of number A on bases/bases p_i, p_j.

Can be formulated the following theorem.

Page 169.

Theorem 4.8. If in the system of bases/bases p_1, p_2, ..., p_n, p_{n+1}, p_{n+2} two bases/bases p_{n+1} and p_{n+2} are control rooms and if the number

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}, \alpha_{n+2}) \quad .$$

is correct, than all projections of number A on bases/bases p_i and p_j are equal to each other and coincide with the value of number A, i.e.

$$A_{ij} = A < \mathcal{P}$$

(with i, j=1, 2, ..., n+2, i≠j) and vice versa, if all projections A_{ij}, numbers A are equal to each other and coincide in the value with number A, then number A is correct.

Proof. Let $A \bar{<} \mathcal{P}$. We form projection on bases/bases p_i and p_j, i.e. A_{ij}. Since

then
$$A_i < \frac{P}{p_i p_j} \; .$$

$$A_{ij} = A_i = A.$$

however, since
$$A < \frac{P}{p_{n-1} p_{n-2}} \cdot \frac{P}{p \cdot p_j} < \frac{P}{p_i} \; .$$

that $A_{ij} = A$ for any values of i and j.

Let us show now that also vice versa, i.e., if all A_j are equal to each other, then A - correct number. Let us first of all show that

$$A_{ij} < \frac{P}{p_{n+1}p_{n+2}} .$$

Since all projections A_{ij} are equal to each other, then, in particular, they are equal to projection $A_{n+1, n+2}$ which is less $\frac{P}{p_{n+1}p_{n+2}}$. Let us assume that A - an incorrect number and in it are erroneous digits α_i and α_j. Let us replace these digits by correct ones $\bar{\alpha}_i$ and $\bar{\alpha}_j$. Let us designate that corrected by digits $\bar{\alpha}_i$ and $\bar{\alpha}_j$ number A through $\bar{A}$. Since $\bar{A}$ - correct number, then all its projections are equal to $\bar{A}$, including projection $\bar{A}_{ij}$. But $\bar{A}_{ij} = A_{ij}$ as composed of one and the same digits on the corresponding bases/bases, therefore, has place and equality

$$\bar{A}_{\rho j} = \bar{A}_{ij} = A_{ij} = A_{\rho j}. \qquad (4.7)$$

where ρ, i, j take values of 0, 1, 2, ..., n+2, moreover $\rho \neq j$, $i \neq j$. Meanwhile if we assume that $\alpha_i \neq \bar{\alpha}_i$, then $\bar{A}_{\rho j}$ and $A_{\rho j}$ consist of identical digits about to all bases/bases, except basis/base p_i, digit on which in them different; therefore (4.7) it is impossible. Hence assumption $\alpha_i \neq \bar{\alpha}_i$ is invalid.

Page 170.

Analogously shows, on the basis of equality $\bar{A}_{i\rho} = A_{i\rho}$, the impossibility of assumption $\alpha_j \neq \bar{\alpha}_j$. Thus, assumption about inaccuracy A is refuted. A is a correct number.

Subsequently we will assume that in the number A accepted can occur only isolated error.

Theorem 4.9. If in system p_1, p_2, ..., p_n, p_{n+1}, p_{n+2} with two control bases/bases is preset incorrect number $\tilde{A} = (\tilde{\alpha}_1, \tilde{\alpha}_2, ..., \tilde{\alpha}_i, ..., \tilde{\alpha}_n, \tilde{\alpha}_{n+1}, \tilde{\alpha}_{n+2})$, then the necessary and sufficient condition of the inaccuracy of digit $\tilde{\alpha}_i$ in $\tilde{A}$ is the correctness of its projection $\tilde{A}_i$ on basis/base p_i. Proof. Let in the incorrect number $\tilde{A}$ be erroneous digit $\tilde{\alpha}_i$, we substitute it by correct α_i. As a result of replacement we obtain the correct number A, whose all projections are equal to each other and are equal to A, i.e., they are correct. Among other things is correct projection A_i. However, since $\tilde{A}_i = A_i$, then $\tilde{A}_i$ is correct; thereby is shown the need for condition.

Let us demonstrate now sufficiency. Let $\tilde{A}$ - incorrect number, but $\tilde{\alpha}_i$ - not erroneous digit. Then erroneous is any another digit, for example $\tilde{\alpha}_j$. Let us note that among all projections of number $\tilde{A}$

$$\tilde{A}_1, \tilde{A}_2, ..., \tilde{A}_i, ..., \tilde{A}_\rho, ..., \tilde{A}_{n+2} \qquad (4.8)$$

there is at least one, which is an incorrect number. Actually/really,
if all these projections were correct, then it would be possible to
write the group of the equalities

$$\tilde{A}_{1, 2} = \tilde{A}_{1, 3} = \ldots = \tilde{A}_{1, n+2};\; \tilde{A}_{2, 1} = \tilde{A}_{2, 3} = \ldots = \tilde{A}_{2, n+2};\; \ldots$$
$$\ldots;\; \tilde{A}_{i, 1} = \tilde{A}_{i, 2} = \ldots = \tilde{A}_{i, n+2};\; \ldots;\; \tilde{A}_{n+2, 1} =$$
$$= \tilde{A}_{n+2, 2} = \ldots = \tilde{A}_{n+2, n+1}.$$

Since in each group there are the coinciding elements/cells, the, all
these projections, which compose the full/total/complete set of the
projections of number $\widetilde{A}$ on any pair of bases/bases, are equal to each
other. In this case of $\widetilde{A}$ must be a correct number. But according to
the condition of present theorem in A is an erroneous digit,
therefore, assumption about the correctness of all projections $\widetilde{A}$ on
any basis/base invalid and among (4.8) is at least one incorrect
number.

Page 171.

Let this be projection $\tilde{A}_p$. We form projection $\tilde{A}_{pi}$, in which is contained
incorrect digit $\tilde{\alpha}_j$. Since $\check{A}_i$ - correct number, then its projection $\tilde{A}_{ip}$
is also a correct number. But $\tilde{A}_{pi} = \tilde{A}_{ip}$, therefore $\tilde{A}_{pi}$ is a correct
number. Let us replace into $\tilde{A}_p$ incorrect digit $\tilde{\alpha}_j$ by correct α_j. We
will obtain $\bar{A}_p$, which is correct, and therefore its projection $\bar{A}_{pi}$ on
basis/base p, is also correct. But $\tilde{A}_{pi}$ and $\bar{A}_{pi}$ as the differing only
in terms of values digits in basis/base p_j cannot simultaneously be

correct. Therefore assumption about the inaccuracy of digit $\tilde{\alpha}_j$ with the correct $\tilde{A}_i$ invalid and error is contained in digit $\tilde{\alpha}_i$. By this is completed the proof of theorem.

From this theorem escape/ensues the following algorithm of the determination of erroneous digit. Are computed the projections of number $\widetilde{A}$ from all bases/bases

$$\tilde{A}_1, \tilde{A}_2, \ldots, \tilde{A}_i, \ldots, \tilde{A}_{n+2}.$$

Among these projections there is one $\tilde{A}_i < \frac{P}{p_{n+1}p_{n+2}}$. Then erroneous is digit $\tilde{\alpha}_i$. After is revealed erroneous digit, its correction is conducted through formula (4.4).

Let us note that the latter/last theorem can be used for the correction not only isolated error, but with some conditions also of double and triple errors.

Let us give the example, which illustrates formulated above algorithm in the system of the bases/bases

$$p_1 = 2; \ p_2 = 3; \ p_3 = 5; \ p_4 = 7; \ p_5 = 11; \ p_6 = 13.$$

Example. Is transmitted number $A = (1, 2, 2, 3, 6, 4) = 17$. Is accepted number $\widetilde{A} = (1, 2, 2, 3, 1, 4)$.

We compute $\widetilde{A}$

$$\tilde{A} = 1 \cdot 15\,015 + 2 \cdot 20\,020 + 2 \cdot 6006 + 3 \cdot 25\,740 + 1 \cdot 16\,380 + 4 \cdot 6930 -$$
$$- r30\,030 = 8207 > 210.$$

The presence of error is established/installed.

Will compute the projections of number $\widetilde{A}$ according to each of the bases/bases.

On basis/base $p_1=2$.

For the system with the bases/bases: $p_2=3$; $p_3=5$; $p_4=7$; $p_5=11$; $p_6=13$ let us compute orthogonal bases $B_2^{(1)} = 5005$; $B_3^{(1)} = 6006$; $B_4^{(1)} = 10725$; $B_5^{(1)} = 1365$; $B_6^{(1)} = 6930$.

Page 172.

Then
$$\tilde{A_1} = (2, 2, 3, 1, 4) = 2 \cdot 5005 + 2 \cdot 6006 + 3 \cdot 10\,725 + 1 \cdot 1365 +$$
$$+ 4 \cdot 6930 - r_1 \cdot 15\,015 = 8207 > 210.$$

On basis/base $p_2 = 3$.

For the system with the bases/bases: $p_1 = 2$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, let us compute the values of the orthogonal bases: $B_1^{(2)} = 5005$. $B_3^{(2)} = 6006$. $B_4^{(2)} = 5720$, $B_5^{(2)} = 6370$, $B_6^{(2)} = 6930$.

Then
$$\tilde{A_2} = (1, 2, 3, 1, 4) = 1 \cdot 5005 - 2 \cdot 6006 + 3 \cdot 5720 + 1 \cdot 6370 +$$
$$+ 4 \cdot 6930 - r_2 10\,010 = 8207 > 210.$$

On basis/base $p_3 = 5$.

We obtain the system: $p_1 = 2$, $p_2 = 3$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$ with the orthogonal bases: $B_1^{(3)} = 3003$, $B_2^{(3)} = 2002$, $B_4^{(3)} = 1716$, $B_5^{(3)} = 4368$, $B_6^{(3)} = 924$.

Whence
$$\tilde{A_3} = (1, 2, 3, 1, 4) = 1 \cdot 3003 + 2 \cdot 2002 + 3 \cdot 1716 + 1 \cdot 4368 +$$
$$+ 4 \cdot 924 - r_3 \cdot 6006 = 2201 > 210.$$

On basis/base $p_4 = 7$.

We have system with the bases/cases: $p_1=2$, $p_2=3$, $p_3=5$, $p_5=11$,

$p_6=13$ and by the orthogonal bases: $B_1^{(4)}=2145$, $B_2^{(4)}=2860$, $B_3^{(4)}=1716$, $B_5^{(4)}=3510$, $B_6^{(4)}=2640$.

Here

$$\tilde{A}_4 = (1, 2, 2, 1, 4) = 1 \cdot 2145 + 2 \cdot 2860 + 2 \cdot 1716 + 1 \cdot 3510 + $$
$$+ 4 \cdot 2640 - r_4 \cdot 4290 = 3917 > 210.$$

On basis/base $p_5=11$.

We will obtain system with bases: $p_1=2$, $p_2=3$, $p_3=5$, $p_4=7$, $p_6=13$.
Orthogonal bases of the system: $B_1^{(5)}=1365$, $B_2^{(5)}=910$, $B_3^{(5)}=546$, $B_4^{(5)}=1170$, $B_6^{(5)}=1470$.

Then

$$\tilde{A}_5 = (1, 2, 2, 3, 4) = 1 \cdot 1365 + 2 \cdot 910 + 2 \cdot 546 + 3 \cdot 1170 + 4 \cdot 1470 - $$
$$- r_5 \cdot 2730 = 17 < 210.$$

On base $p_6=13$.

System has bases/bases: $p_1=2$, $p_2=3$, $p_3=5$, $p_4=7$, $p_5=11$ and the

orthogonal bases: $B_1^{(6)}=1155$; $B_2^{(6)}=1540$; $B_3^{(6)}=1386$; $B_4^{(6)}=330$; $B_5^{(6)}=210$.

Then

$$\tilde{A}_6 = (1, 2, 2, 3, 1) = 1 \cdot 1155 + 2 \cdot 1540 + 2 \cdot 1386 + 3 \cdot 330 + $$
$$+ 1 \cdot 210 - r_6 2310 = 1277 > 210.$$

Thus, all projections of number $\tilde{A}$, except $\tilde{A}_5$ are incorrect.
Consequently, is erroneous infra $a_5=1$ on base $p_5=11$.

Let us lead now correction according to formula (4.4) for

projection A_5:

$$\alpha_5 = 1 - \left[\frac{11(1-13)}{13} - \frac{8207}{1365} \right] = 6;$$

Correct digit on base 11 is equal to $\alpha_5 = 6$.

Page 173.

From the character of examined codes is visible their
full/total/complete arithmetic nature - introduced additionally bases
are connected with the general/common/total system of bases/basis and
the codes, containing digits on all both basic and check bits, they
participate in any operation of arithmetic unit, processing of basic
and further digits it is produced completely in an identical way,
without any difference. This makes it possible to consider that
processing the information, represented in of this type the special
code, can be conducted without the check of each single code, and it
is only step by step, the value of each stage can be determined in
each individual case, either on fore-and-aft cycle of processing or
in the conformity with probability of the emergence of isolated
error. The final result of each stage can be subjected to check and
its correctness confirms the correctness of the carrying out of all
operations of this stage.

In the case of the detection of the error is produced the
correction and corrected result participates in the subsequent

stages. Possibility of this mode/conditions of processing the information is equivalent to double error for detection of error and to triple error for its correction.

It is interesting to note that the introduction only of one control basis/base, proves to be, make it possible to discover not only any isolated error (in the digit on one base) but also 95o/o of double ones (in the digits of two bases/bases).

§4.4. Questions of the control of arithmetic operations.

Almost all elementary arithmetic operations can be considered as two-component. Let us designate the i-th elementary operation through E_i, and its components - through A_i and B_i let us register operation in the form

$$E_i = f_i (A_i, B_i)$$

(in particular, can occur $A_i = B_i$).

Let us name circuit F the set of the operations above components $a_1, a_2, \ldots, a_m$ —

$$F (a_1, a_2, \ldots, a_m),$$

which can be represented in the form of the superposition of such two-component operations with the possible repetitions both of very a_j, and intermediate results of executing the two-component

operations.

Page 174.

It is assumed that in the circuit of operations there are no interruptions/discontinuities, understanding under this the fact that, with exception of final result, there exists no intermediate result which subsequently would not enter as the component at least into one two-component operation.

Thus, for instance

$$F(a_1, a_2, \ldots, a_m) = a_1 a_2 + a_2 a_3 + \ldots + \ldots + a_{m-1} a_m$$

is circuit in that sense as this was determined above. Actually/really, it is possible F to register in the form of the superposition of the two-component operations

$$F = f_2 \{ \ldots f_2 \{ f_2 [f_1(a_1, a_2), f_1(a_2, a_3)], f_1(a_3, a_4) \} \ldots \},$$

where f_1 - operation of multiplication, f_2 - addition.

Logical to introduce into determination of circuit stipulation, that precisely the result of calculation all over circuit is the final interesting us result, but all others, which are formed in the course of calculations, intermediate results, which do not have independent value and us interesting inasmuch as they participate in the formation of final result. Therefore, if in the intermediate

results are contained the errors, which can be corrected as a final
result, it is possible to be bounded to the correction only of this
latter/last result, without being converted to the history of its
obtaining and without producing the restoration/reduction of the true
values of intermediate results. In other words during the work of
computer must be provided obtaining the true value only of the final
result of calculating the circuit.

Additionally is put forth the following assumption: in the
implementation of circuit can occur the error only in the digit of
one basis/base, i.e., length of chain is such, that with the existing
characteristics of the reliability of the work of the equipment for
arithmetic unit is probable the presence of short duration failure or
failure only on one of the bases/bases. With this unimportantly,
whether occurred on this basis/base single short duration failure or
occurred several failures.

Under the assumptions presented the state of the final result of
circuit is characterized as follows.

Page 175.

Let be implemented a certain circuit of rational operations whose
true result in the case of the absence of the errors in the course of

calculations must be a correct number, and let in the process of calculation occur one or several short duration failures on one of the basis of system. Then the final result of circuit either incorrect or true.

Actually/really, let be is accepted the representation representation in the systems of bases/bases $p_1, p_2, \ldots, p_n, p_{n+1}$ and true result must be number $K = (x_1, x_2, \ldots, x_i, \ldots, x_{n+1})$, and is obtained number $A = (\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_{n+1})$. If short duration failure they occurred on base p_i, then

$$\alpha_1 = x_1, \alpha_2 = x_2, \ldots, \alpha_{i-1} = x_{i-1}, x_{i+1} = x_{i+1}, \ldots, \alpha_{n+1} = x_{n+1}$$

Concerning α_i, then the possible two versions
1) $\alpha_i \neq x_i$;
2) $\alpha_i = x_i$.

In version 1 number A is incorrect in version 2 number A correct and in this case coinciding with K, i.e., A is the true value of the final result of circuit.

Established fact, it would seem very simple, it has, however, important value for organization of control in the computer, which works in the system of residual classes. It attests to the fact that in the final result of calculating the circuit cannot penetrate the undetected error, since thiss could occur only when the result of calculations would be correct, but at the same time not true number. However, correct number can be only true result.

Thus, error, if it in any stage of the realization of circuit
occurred, either will be preserved to the end of the calculation of
circuit and will show itself by the easily detected inaccuracy of
final result or in the process of further, after its emergence,
calculations it will self-eliminate and then is obtained necessary
final result.

The withdrawal of error can occur not only in the case of the
imposition of several short duration failures on this basis/base, but
also with the single short duration failure.

Page 176.

Thus, for instance, if in any stage of the calculation of circuit
already after the emergence of short duration failure on basis/base
$\bar{p}_i$ intermediate result was multiplied by the number, which has zero
digit on $\bar{p}_i$, then, obviously, product will be obtained the true number
and the same already it will enter into the subsequent calculations,
which in the absence subsequently of short duration failures,
naturally, will lead to obtaining of true final result.

Until now, speaking about the rational operations, bore in mind

MICROCOPY RESOLUTION TEST CHART
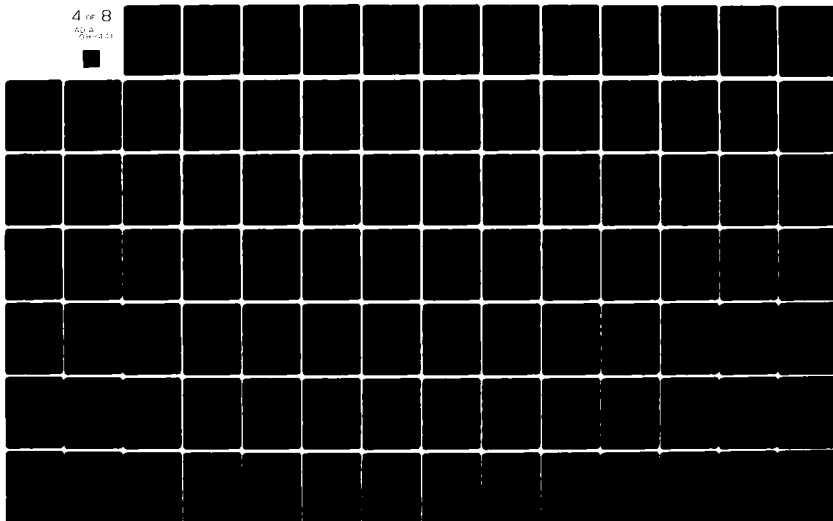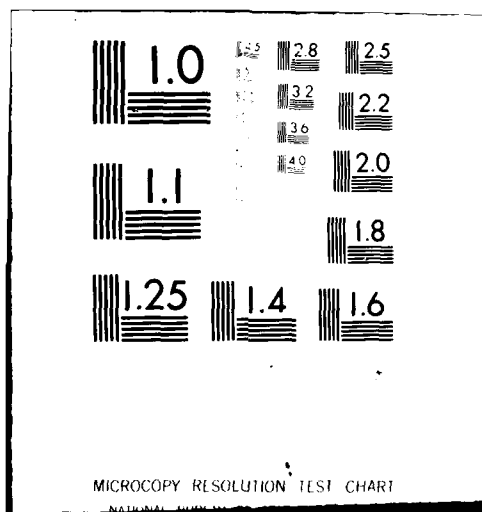
the operation of addition, suttraction, multiplication and the cases
of the step-by-step implemented division when divided multiply to
divider/denominator are absent critical situations in the form of
zero digits in the divider/denominator.

Somewhat apart among these operations from the point of view of
control is located strictly the operation of the machine approximate
division in general. As we saw, in the implementation of the various
kinds of the algorithms, connected with the division, the dominant
role plays the operation of division into the basis of system.

Let us consider how is reflected in the quotient the presence of
the error in the dividend with the execution of this operation.

Assume we should obtain quotient $C = A : p_j$, where
$A = (\alpha_1, \alpha_2, \ldots, \alpha_j, \ldots, \alpha_{n+i})$. Since in the system of residual classes
division must be implemented only completely, the dividend must be
multiple to divider/denominator, i.e., have zero digit on base p_j.
Therefore, if $\alpha_j \neq 0$, then instead of A as the dividend is taken

$$A_{\text{дел}} = A - \alpha_j,$$

that being close to A multiple p_j number. Then

$$C = \frac{A_{\text{дел}}}{p_j} = (\gamma_1, \gamma_2, \ldots, \gamma_{j-1}, \gamma_j, \gamma_{j+1}, \ldots, \gamma_{n+i}),$$

where

$$\gamma_{i \neq j} = \frac{\alpha_i + p_j - \alpha_j}{p_j} \pmod{p_i},$$

and γ_j - the digit of quotient on p_j is determined on one of the methods, presented in Chapter 3. It is important to note that any of these methods in this or other form considers the values of all digits $A_{\text{нел}}$.

If in the process of calculation A occurred the error and instead of A in the calculations figures number $\widetilde{A} = (\alpha'_1, \alpha'_2, \ldots, \alpha'_j, \ldots, \alpha'_{n+1})$, then as the dividend will be accepted the number

$$\widetilde{A}_{\text{нел}} = \widetilde{A} - \alpha'_j$$

and quotient will prove to be equal.

Page 177.

$$\widetilde{C} = \frac{\widetilde{A}_{\text{нел}}}{p_j} = (\gamma'_1, \gamma'_2, \ldots, \gamma'_j, \ldots, \gamma'_{n+1}).$$

If in $\widetilde{A}$ is an error on one of bases/bases p_j, then this error in different ways will be reflected in the quotient in cases when $i \neq j$ and $i = j$. Let us examine them.

Case 1. Let $i \neq j$. Occur the relationships/ratios

$$\gamma'_1 = \gamma_1; \ \gamma'_2 = \gamma_2; \ \ldots; \ \gamma'_{i-1} = \gamma_{i-1}; \ \gamma'_{i+1} = \gamma_{i+1}; \ \ldots$$
$$\ldots; \ \gamma'_{j-1} = \gamma_{j-1}; \ \gamma'_{j+1} = \gamma_{j+1}; \ \ldots; \ \gamma'_{n+1} = \gamma_{n+1}.$$
$$\gamma'_i \neq \gamma_i, \ \gamma'_j \neq \gamma_j.$$

The here obtained quotient, as a rule, differs from true in digits already in two bases/bases:

- on base p_i, since in the dividend was erroneous digit α_i, what, naturally, involved inaccuracy $\dot{\gamma}_i$, and

- on base p_j, since in view of the presence of erroneous digit α_i in $\widetilde{A}$ there will be, generally speaking, is erroneously determined digit γ_j. Exception/elimination they can compose such errors in p_i, which do not vary the digit of quotient on p_j. This is possible with very special combinations of digits $\widetilde{A}$ which are encountered sufficiently rarely.

Thus, the quotient $\widetilde{c}$ is already containing errors on two bases, what exceeds the scope of the examined/considered by us situation - the assumption that the error in numbers affects only one basis/base. Furthermore, quotient can prove to be the correct number, although which differs in terms of two digits from true.

Case of 2. Let i=j. Here picture sharply varies.

$$\gamma_1' \neq \gamma_1; \ \gamma_2' \neq \gamma_2; \ \dots; \ \gamma_{j-1}' \neq \gamma_{j-1}; \ \gamma_{j+1}' \neq \gamma_{j+1}; \ \dots$$
$$\dots; \ \gamma_{n+1}' \neq \gamma_{n+1}.$$

For the digit of quotient on basis/base p_j it can be

or
$$\gamma_j' \neq \gamma_j$$
$$\gamma_j' = \gamma_j.$$

Page 178.

In view of the fact that due to the inaccuracy of digit α_j incorrectly is formed $\tilde{A}_{\text{лен}}$ on all digits, they prove to be incorrect and all digits of quotient, with exception, perhaps, only digit p_j', which during some combinations of digits $\tilde{A}_{\text{лен}}$ can prove to be that coinciding with γ. In this case the quotient can prove to be a correct number.

Thus, case of 2 leads to the quotient in which the error distribution even more differs from the accepted by us assumption about the inaccuracy of digit only in one basis/base.

Questions of the development/detection of a similar kind of multiple errors and their correction require special research. Certain assistance in the solution of this question can render the following theorem.

Theorem 4.10. If during the division of incorrect number $\tilde{A}_{\text{лен}}$ into basis/base p_j quotient $\tilde{C} = \dfrac{\tilde{A}_{\text{лен}}}{p_j}$ was obtained by a correct number, then when $p_j' < p_{n+1}$ digit α_j' cannot be erroneous.

Proof. Actually/really, if occurred into A error on base p_j, then

$$\tilde{A} > \frac{P}{p_j}.$$

In this case the quotient

$$\tilde{C} = \frac{A_{\text{дел}}}{p_j} > \frac{P}{p_j^2} > \frac{P}{p_{n+1}}$$

must be an incorrect number. Since $\tilde{C}$ according to the condition of theorem - correct number, proves to be invalid the assumption about inaccuracy a_j.

From this theorem escape/ensues preference, in the known sense, small bases/bases as the dividers/denominators during the organization of division.

§4.5. Alternating nature of correction with one surplus basis/base.

Generally speaking for the correction of the error for the introduction only of one surplus basis/base it is insufficient. However, there are cases, when in the presence only of one control basis/base nevertheless it is possible to unambiguously establish/install erroneous digit.

Page 179.

It is earlier, speaking about the possibility to be bounded to control and correction only of the final result of calculation, we they had in mind the presence of that entire redundancy in the code representation, that was necessary for the correction isolated/insulated the undertaken number.

Let us now lead detailed research of the possibilities of organizing the correction in the presence only of one surplus basis/base in the section/cut of the dynamics of computational process, i.e., by examining the character of error distribution in the results, consecutively/serially obtained in the implementation of program.

Determination. Let us name this incorrect number $\tilde{A}$ a k-alternatively corrected (or simply k-alternative) number, if there are k of such correct numbers $A_1, A_2, \ldots, A_k$, each of which differs from $\tilde{A}$ in terms of digit of any one basis/base, moreover these bases are different for different A_ρ $(\rho = 1, 2, \ldots, k)$.

The set of bases/bases $(p_{i_1}, p_{i_2}, \ldots, p_{i_k})$, in which numbers $A_1, A_2, \ldots, A_k$ differ from $\tilde{A}$, let us name the alternative set of number $\tilde{A}$ and we will designate $\mathfrak{A}(\tilde{A})$.

Let us note that basis/base p_{n+1} always enters into the

alternative set of any number $\tilde{A}$. Actually/really, whatever first n of

the digits of number $\tilde{A}$, there is always this digit on basis/base p_{n+1},

that the number, which has on basis/base p_{n+1} digit ξ, lies/rests in

the range $\left[0, \frac{p}{p_{n+1}}\right)$, being a correct number.

From this circumstance it is possible to do, in particular, a

conclusion about the advisability of increase in the implementation

of arithmetic units by purely technical means of the higher

reliability of operation precisely of those diagrams, which are

realized operations on basis/base p_{n+1}. During this organization of

work of the arithmetic units when the error in basis/base p_{n+1} is

unlikely and, therefore, base p_{n+1} can not be built-in into the

alternative set frequently it can seem that the alternative set will

consist of one basis/base and the correction of result will be

simplified.

Alternative set $\mathfrak{A}(\tilde{A})$ of number $\tilde{A}$ can be

established/installed by testing each of the bases/bases p_i (i=1, 2,

..., n+1) as follows.

Page 180.

Are computed all possible values of number A_ρ, is determined the

sequence of the numbers, which have one and the same digits on all
bases/bases, as number $\tilde{A}$, besides base p_p, and differing only in terms
of digits in this base, i.e., the number

$$A_{ps} = (\alpha_1', \ldots, \alpha_{p-1}', S, \alpha_{p+1}', \ldots, \alpha_n', \alpha_{n+1}'),$$
$$S = 0, 1, \ldots, p_p - 1.$$

Among these a number it can not be one correct number, or there
can be only one correct number. In the latter case p_p it enters into
the alternative set of number $\tilde{A}$. After leading analogous testings for
each of the basis of system, we determine completely $\mathfrak{A}(\tilde{A})$.

This way of determining the alternative set of a number $\tilde{A}$ is
sufficiently labor-consuming and subsequently will be given more
efficient method.

Let us preliminarily consider the example, which illustrates the
concept of alternative set in the system with the bases/bases

$$p_1 = 2; \quad p_2 = 3; \quad p_3 = 5; \quad p_4 = 7; \quad p_5 = 11.$$

Example. To determine the alternative set of the number

$$\tilde{A} = (1, 2, 2, 5, 6) = 677 > 210.$$

It is checked basis/base $p_1 = 2$. We compute the value
$A_{10} = (0, 2, 2, 5, 6).$

$$A_{10} = 0 \times 1155 + 2 \times 1540 + 2 \times 1386 + 5 \times 330 + 6 \times 210 -$$
$$- r_{A_{10}} \cdot 2310 = 1832 > 210.$$

Consequently, $p_1 = 2$ does not enter in $\mathfrak{A}(\tilde{A})$.

Is checked basis/base $p_2 = 3$. We compute A_{20} and A_{21}.

$$A_{20} = (1, 0, 2, 5, 6) = 2217 > 210, \quad A_{21} = (1, 1, 2, 5, 6) = 1447 > 210.$$

Basis/base $p_2=3$ also does not enter in $\mathfrak{A}(\widetilde{A})$.

It is checked basis/base $p_3=5$. We compute values of A_{30}, A_{31}, A_{33} and A_{34}:

$$A_{30}=(1, 2, 0, 5, 6)=215 > 210, \quad A_{31}=(1, 2, 1, 5, 6)=1601 > 210,$$
$$A_{33}=(1, 2, 3, 5, 6)=2063 > 210, \quad A_{34}=(1, 2, 4, 5, 6)=1139 > 210.$$

Basis/base $p_3=5$ does not enter in $\mathfrak{A}(\widetilde{A})$.

It is checked basis/base $p_4=7$. Let us calculate values A_{40}, A_{41}, A_{42}, A_{43}, A_{44}, A_{46}.

$$A_{40}=(1, 2, 2, 0, 6)=1337 > 210, \quad A_{43}=(1, 2, 2, 3, 6)=17 < 210,$$
$$A_{41}=(1, 2, 2, 1, 6)=1667 > 210, \quad A_{44}=(1, 2, 2, 4, 6)=347 > 210,$$
$$A_{42}=(1, 2, 2, 2, 6)=1997 > 210, \quad A_{46}=(1, 2, 2, 6, 6)=1007 > 210.$$

Page 181.

Base $p_4=7$ enters in $\mathfrak{A}(\widetilde{A})$; and if error occurred precisely on base p_4, then the true digit of number $\widetilde{A}$ on this foundation for eating 3.

In accordance with that presented above into alternative set enters also basis/base $p_5=11$. Thus, number $\widetilde{A}$ is a two-alternative number and the alternative set of number $\widetilde{A}=(1, 2, 2, 5, 6)$ is defined as $\mathfrak{A}(\widetilde{A})=(7, 11)$.

Let us consider the theorems, somewhat inswept the field of the

searches for the alternative set of a number.

Theorem 4.11. Let be preset the regulated system of the bases/bases

$$p_1, p_2, \ldots, p_n, p_{n+1}$$

and let incorrect number $\widetilde{A} = (\alpha_1', \alpha_2', \ldots, \alpha_n', \alpha_{n+1}')$ satisfy inequality $\frac{P}{p_{n+1}} < \widetilde{A} < \frac{P}{p_j}$. Then bases/bases $p_1, p_2, \ldots, p_j$ do not enter into alternative set $\mathfrak{A}(\widetilde{A})$ of number $\widetilde{A}$.

This theorem although gives the possibility to narrow down the framework of the search for the alternative set of number $\widetilde{A}$ upon the satisfaction to inequality $\widetilde{A} < \frac{P}{p_j}$, it makes it possible to make no conclusions in the case $\widetilde{A} > \frac{P}{p_i}$ relative to that, does enter p_j in $\mathfrak{A}(\widetilde{A})$. Therefore let us formulate and will demonstrate fuller/more total/more complete theorem.

Theorem 4.12. Let be preset the regulated system of the bases/bases

$$p_1, p_2, \ldots, p_n, p_{n+1}$$

and let be is preset the incorrect number $\widetilde{A}$ whose projection on foundation for p_i eating $\widetilde{A}_i$. Then the necessary and sufficient condition of entrance p_i into alternative set $\mathfrak{A}(\widetilde{A})$ is the correctness of projection $\widetilde{A}_i$.

Proof. Actually/really, let us suppose projection $\tilde{A}_i$ is a correct number.

Page 182.

Since among the sequence of numbers $\tilde{A}_{i,0}, \tilde{A}_{i,1}, \ldots, \tilde{A}_{i,p_i-1}$ is always contained number $\tilde{A}_{i\xi}$, is smaller $\frac{P}{p_i}$, this number is equal to projection $\tilde{A}_i$, since projection $\tilde{A}_i$, through supposition, is located in the range $\left[0, \frac{P}{p_i}\right)$ and digits $\tilde{A}_i$ coincide with appropriate digits (with exception, naturally, digits in base p_i).

All numbers of sequence differ from $\tilde{A}_{i\xi}$ to different multiple ones $B_i = \frac{m_i P}{p_i}$, _i.e._, any number of this sequence, in the rate and $\vec{A} = \tilde{A}_{i,\alpha_i'}$, it can be registered in the form

$$\tilde{A} = km_i \frac{P}{p_i} + \tilde{A}_{i\xi} = K \frac{P}{p_i} + \tilde{A}_{i\xi} = K \frac{P}{p_i} + \tilde{A}_i.$$

Here $km_i = lp_i + K$ is substituted on K, since

$$lp_i \frac{P}{p_i} = lP$$

comprises a number, multiple to the range P accepted. It is obvious, K to eat nothing else but integer part of division of $\tilde{A}$ on $\frac{P}{p_i}$ and, therefore,

$$\tilde{A}_{i\xi} = \tilde{A}_i = \tilde{A} - \left[\frac{\tilde{A}p_i}{P}\right] \frac{P}{p_i}. \qquad (4.9)$$

Thus, if $\tilde{A}_i$ — correct number, then among numbers $\tilde{A}_{i0} \ldots \tilde{A}_{i,p_i-1}$ is contained number $\tilde{A}_{i\xi}$, which is a correct number, i.e., p_i enters into

the alternative set of number $\bar{A}$. By this is established/installed the sufficiency of condition.

Let us now show its necessity. Let p_i enter in $\mathfrak{A}(\tilde{A})$. Then among the sequence of numbers $\tilde{A}_{i_0} \cdots \tilde{A}_{i_1 p_i - 1}$ must be contained correct, i.e., is smaller P/p_{n+1}, a number. This can be only $\tilde{A}_{i_\xi} < P/p_i$, since each of the remaining numbers of sequence is more than P/p_i and is as of old more than P/p_{n+i}. But $\tilde{A}_{i_\xi} = \tilde{A}_i$. Consequently, $\tilde{A}_i$ must be a correct number.

Let us use the proved theorem to the solution of the previous example.

Example. To determine the alternative set of the incorrect number $\tilde{A} = (1, 2, 2, 5, 6) = 677 > 210$.

Page 183.

We compute the projections of number $\tilde{A}$ according to formula (4.9):

$$A_1 = 677 - \left[\frac{677 \cdot 2}{2310}\right] \frac{2310}{2} = 677 > 210,$$

$$A_2 = 677 - \left[\frac{677 \cdot 3}{2310}\right] \frac{2310}{3} = 677 > 210,$$

$$A_3 = 677 - \left[\frac{677 \cdot 5}{2310}\right] \frac{2310}{5} = 677 - 462 = 215 > 210,$$

$$A_4 = 677 - \left[\frac{677 \cdot 7}{2310}\right] \frac{2310}{7} = 677 - 2 \cdot 330 = 17 < 210,$$

$$A_5 = 677 - \left[\frac{677 \cdot 11}{2310}\right] \frac{2310}{11} = 677 - 3 \cdot 210 = 47 < 210.$$

Into alternative set numbers $\tilde{A}$ enter bases 7 and 11

$$\mathfrak{A}(\hat{A}) = (7, 11).$$

it is here expedient to again emphasize that when the incorrect
number $\tilde{A}$ undergoes subsequently to different rational operations with
the enlistment of other numbers (predicted correct ones), then the
results of these operations will be either true or incorrect,
moreover in the latter case of erroneous there will be digit on that
basis/base, on which there was an error in $\tilde{A}$. In other words as a
result of the fulfillment of sequence of operations with the
participation of the incorrect number $\tilde{A}$ the error can either be
reduced or remain on the spot, but by no means it cannot move into
the digit on one or another basis/base. However, as far as aggregate
of the results is concerned alternative of operations, then it can
differ significantly from the alternative set $\tilde{A}$.

Let us consider changes in the alternative aggregates of the
results of arithmetic operations. In this case we will be guided by
the following agreement.

Agreement. In the circuit of the operations, implemented by op
to real program, the latter is constructed in such a way that all
intermediate results, just as final result, in the case of the
absence of the errors in the course the implementations of program
are correct numbers.

This condition is completely logical for the correctly
constructed program, since preliminary scaling must ensure the
nonappearance of the results of calculations beyond the limits of
operating range.

Page 184.

Determination. We will call the arithmetic operation of correct,
if operands and result of operation are correct numbers.

However, concerning our direct target - carrying out of
correction, the for it formulated condition it can make that sense,
that, after taking hypothetically any of the alternatives for the
true and after leading correction in the conformity with this
hypothesis, we in further course of the program must discover the
unsoundness of the incorrect hypothesis, i.e., to obtain on some one
from the subsequent stages an incorrect number. It is obvious, in
this case it is assumed that the test of hypothesis is produced
during the period when is excluded the possibility of the emergence
of new short duration failure.

Let us consider the following theorem about the character of the

alternative aggregate of the results of operation.

Theorem 4.13. If in the regulated system of the bases/bases

$$p_1, p_2, \ldots, p_n, \widetilde{p}_{n+1}$$

is preset the incorrect number $\widetilde{A}$, which has the alternative set

$$\mathfrak{A}(\widetilde{A}) = (p_{i1}, p_{i2}, \ldots, p_{ih}),$$

and if with the execution on number $\widetilde{A}$ of rational operation according

to the program obtained the incorrect number $\widetilde{B}$ whose alternative set

was equal to

$$\mathfrak{A}(\widetilde{B}) = (\overline{p}_{i1}, \overline{p}_{i2}, \ldots, \overline{p}_{i\alpha}),$$

then erroneous there can be digit on any of the bases/bases

$$(p_{j1}, p_{j2}, \ldots, p_{j\bullet}) = \mathfrak{A}(\widetilde{A})\,\mathfrak{A}(\widetilde{B}),$$

where the multiplication is understood in the sense of intersection.

Proof. Let us first of all note that among the the alternative

sets $\mathfrak{A}(\widetilde{A})$ and $\mathfrak{A}(\widetilde{B})$, is always contained basis/base p_i, on which occurred

the error. Thus, if in $\mathfrak{A}(\widetilde{A})$ there are such bases/bases, which are not

in $\mathfrak{A}(\widetilde{B})$, and vice versa, then, obviously, among such bases/bases is not

present basis/base p_i - it can be only among those bases/bases, which

are general/common/total for $\mathfrak{A}(\widetilde{A})$ and $\mathfrak{A}(\widetilde{B})$, among intersection.

Page 185.

Definition. By conditional alternative set $\widetilde{\mathfrak{A}}(\widetilde{A})$ of the incorrect

number $\widetilde{A}$ we will understand the set of bases/bases, on which is possible the error, taking into account the character of the alternative sets of the previous incorrect results on the course of executing the program.

If consecutively/serially were obtained the incorrect numbers

$$\widetilde{A}_1, \widetilde{A}_2, \ldots, \widetilde{A}_\rho,$$

that

$$\widetilde{\mathfrak{A}}(\widetilde{A}) = \mathfrak{A}(\widetilde{A}_1)\,\mathfrak{A}(\widetilde{A}_2) \ldots \mathfrak{A}(\widetilde{A}_\rho)$$

or in the recurrent form

$$\widetilde{\mathfrak{A}}(\widetilde{A}_\rho) = \widetilde{\mathfrak{A}}(\widetilde{A}_{\rho-1})\,\mathfrak{A}(\widetilde{A}_\rho).$$

To the expressed above assumption that the reception of wrong hypothesis from the alternative set must with the large probability lead to the incorrect result and which thereby only valid hypothesis ensures the correctness of results in all stages, in the terms of alternative sets it corresponds assertion, which with the same degree of probability in view of the occurring consecutive judgment of the conditional alternative aggregates of the results of operations exists such ρ, with which

$$\widetilde{\mathfrak{A}}(\widetilde{A}_\rho) = (p_1),$$

where p_i - the basis/base on which occurred the error during calculation $\widetilde{A}$. These two judgments could be considered equivalent, if not the fact that surplus basis/base p_{n+1} always enters in $\mathfrak{A}(\widetilde{A}_\rho)$ and, therefore, whatever was conducted as results of sequence of

operations the contraction of conditional alternative set to
erroneous base p_n nevertheless there will together with p_i figure
also p_{n+1}.

Page 186.

In accordance with that presented it is the possible to
determine several methods of organizing of control and correction of
the errors:

- one path consists in the consecutive determinations of
conditional alternative sets in the course of execution of program
and their contraction to the erroneous basis/base;

- another path consists of the reception of any hypothesis on
the alternative set of number $\tilde{A}$, the carrying out of correction on
this hypothesis and the execution of further calculations until the
detection of the groundlessness of the hypothesis accepted and
transition to another hypothesis. If in this case the groundlessness
of the hypothesis accepted is not showed, then the obtained results
are accepted for the true ones;

- is feasible and the third path - synthesis the first two
methods. Are computed conditional alternative sets a number, that are

obtained in proportion to the implementation of program, up to their
contraction in number A_p to bases/bases p_i and p_{n+1}, after which is
accepted the hypothesis of the inaccuracy of digit on base p_i and is
conducted its correction in number $\bar{A}_p$. The detection of the
groundlessness of this hypothesis determines the inaccuracy of digit
on basis/base p_{n+1}.

About to the methods of conducting the correction proposed it is
necessary to do the following observations:

- in all cases it is assumed that the realizable circuit of
operations possasses a sufficient length, which allows performance of
all intended procedures to the exhaustion of the operations of
circuit;

- for all methods desirably to obtain either probabilistically
analytical or simulation the evaluation of the period (in quantities
of operations) of the stable realization of procedures (contraction
of conditional alternative sets, disproof or the confirmation of
hypothesis, etc.);

- in the case of receiving the erroneous hypothesis when
correction is not substantiated carried out on basis/base p_i while
erroneous is p_i, a number proves to have already two errors: on known

basis/base p_j, as a result of the introduced by correction distortion and on to be determined base p_i, where the error actually arose as a result of short duration failure. In this case is required return to an erroneous number.

Let us consider some examples in the system with the bases/bases

$$p_1 = 2;\ p_2 = 3;\ p_3 = 5;\ p_4 = 7;\ p_5 = 11.$$

Example. Let us compute the value of function Y=2x.

Let on the previous stage be is calculated the value

$$x = (1,\ 1,\ 3,\ 1,\ 1) = 463 > 210.$$

Page 187.

Number x is incorrect. We determine its alternative set:

$$A_1 = 463 - \left[\frac{463 \cdot 2}{2310}\right] \frac{2310}{2} = 463 > 210,$$

$$A_2 = 463 - \left[\frac{463 \cdot 3}{2310}\right] \frac{2310}{3} = 463 > 210,$$

$$A_3 = 463 - \left[\frac{463 \cdot 5}{2310}\right] \frac{2310}{5} = 463 - 462 = 1 < 210,$$

$$A_4 = 463 - \left[\frac{463 \cdot 7}{2310}\right] \frac{2310}{7} = 463 - 330 = 133 < 210,$$

$$A_5 = 463 - \left[\frac{463 \cdot 11}{2310}\right] \frac{2310}{11} = 463 - 420 = 43 < 210,$$

one

$$\mathbf{u}(x) = (5,\ 7,\ 11).$$

We compute value of Y=2x:

$$Y = (0, 2, 2, 2, 2)(1, 1, 3, 1, 1) = (0, 2, 1, 2, 2) = 926 > 210.$$

Analogous with previous we determine:

$$A_1 = 926 > 210, \quad A_2 = 156 < 210, \quad A_3 = 2 < 210,$$
$$A_4 = 266 > 210, \quad A_5 = 86 < 210,$$
$$\mathfrak{A}(Y) = (3, 5, 11).$$

Then conditional alternative set is defined as

$$\widetilde{\mathfrak{A}}(Y) = (3, 5, 11)(5, 7, 11) = (5, 11).$$

Thus, erroneous is digit either on base $p_3 = 5$ or on base $p_5 = 11$. If error does not contain digit or basis/base $p_5 = 11$, then further convolution of conditional alternative set in the process of the subsequent operations it is impossible.

Let us consider, that gives under conditions of the example in question reception of hypothesis about the erroneous digit in number x before the calculation of value of Y.

1. We assume that erroneous was digit on basis/base $p_3 = 5$. We carry out correction x. We obtain

$$\overline{x} = (1, 1, 1, 1, 1) = 1.$$

We compute

$$\overline{Y} = 2\overline{x} = (0, 2, 2, 2, 2) = 2 < 210.$$

The groundlessness of hypothesis was not discovered.

2. We accept inaccuracy of digit on base $p_4 = 7$. We obtain

$$\overline{x} = (1, 1, 3, 0, 1) = 133,$$
$$\overline{Y} = 2\overline{x} = (0, 2, 1, 0, 2) = 266 > 210.$$

Is discovered the groundlessness of the hypothesis accepted.
Digit on basis/base $p_4 = 7$ cannot be erroneous.

Page 198.

3. Let us take now erroneous digit on base $p_5 = 11$ we will obtain

$$\bar{x} = (1, 1, 3, 1, 10) = 43,$$
$$\overline{Y} = 2\bar{x} = (0, 2, 1, 2, 9) = 86 < 210.$$

The inaccuracy of hypothesis is not confirmed.

Under conditions of this example both methods led to one and the same result — was excluded the inaccuracy of digit on basis/base $p_4 = 7$.

Thus, this simple operation, kA the doubling of a number, made it possible to narrow down the framework of the search for erroneous digit.

Example. Is computed the value of function $Y = 6x$. Number x the same as in the previous example, and $\mathfrak{A}(x) = (5, 7, 11)$.

We compute

$$Y = 6\bar{x} = (0, 0, 1, 6, 6)(1, 1, 3, 1, 1) = (0, 0, 3, 6, 6) = 468 > 210.$$

We determine:

$$A_1 = 468 > 210, \; A_2 = 468 > 210, \; A_3 = 6 < 210,$$
$$A_4 = 138 < 210, \; A_5 = 48 < 210,$$
$$\mathfrak{A}(Y) = (5, 7, 11).$$

Conditional alternative set is defined as

$$\widetilde{\mathfrak{A}}(Y) = (5, 7, 11)(5, 7, 11) = (5, 7, 11).$$

It no new information about the possible localization error obtains.

To other entirely results it leads correction method on the hypotheses.

1. We accept erroneous digit on basis/base $p_3 = 5$. The correction of digit on this basis/base brings to

$$\overline{Y} = 6\overline{x} = (1, 1, 1, 1, 1)(0, 0, 1, 6, 6) = (0, 0, 1, 6, 6) = 6 < 210.$$

2. We accept erroneous digit on base $p_4 = 7$. This it gives

$$\overline{Y} = 6\overline{x} = (0, 0, 1, 6, 6)(1, 1, 3, 0, 1) = (0, 0, 3, 0, 6) = 798 > 210.$$

Consequently, on foundation for $p_4 = 7$ of error being it cannot.

3. Finally, it is permitted inaccuracy of digit on base $p_5 = 11$. This it gives

$$\overline{Y} = 6\overline{x} = (0, 0, 1, 6, 6)(1, 1, 3, 1, 10) = (0, 0, 3, 6, 5) = 258 > 210.$$

Thereby is excluded the possibility of errors also on basis/base p_5. Remains only possibility - error it took place on basis/base $p_3 = 5$ and true value Y is (0, 0, 1, 6, 6).

For purposes of the decrease of the capacity of conditional alternative set and realization of its more rapid contraction to actually erroneous base can prove to be highly useful the following theorems of particular character.

Page 189.

Theorem 4.14. Let in the regulated system of the bases/bases

$$p_1, p_2, \ldots, p_n, p_{n+1}$$

be is preset the incorrect number

$$\tilde{A} = (\alpha_1', \alpha_2', \ldots, \alpha_i', \ldots, \alpha_n', \alpha_{n+1}'),$$

moreover it is known that basis/base p_i enters into alternative set $\mathfrak{A}(\tilde{A})$ of number $\tilde{A}.$ Then if in the product

$$\tilde{C} = B\tilde{A},$$

where B - correct number with the zero digit on base p_i, will prove to be that $\tilde{C}$ - incorrect number, digit α_i on base p_i is not erroneous.

Proof. Actually/really, if digit α_i would be erroneous, then in $\tilde{C}$ this error must self-eliminate, since regardless of the fact which digit α_i' in $\tilde{C}$, it gives on basis/base p_i zero, and $\tilde{C}$ must be a correct number. But $\tilde{C}$ proved to be an incorrect number. Consequently, α_i' - correct digit.

On the basis of this theorem basis/base p_i can be excluded from

$\cdot \mathfrak{A}(\widetilde{C})$, if it there enters.

Example. Number $\tilde{A}=(1,\ 2,\ 2,\ 5,\ 6)$ has alternative set $\mathfrak{A}(\widetilde{A})=(7,11)$.

As the multiplier let us take number $B=(1,\ 2,\ 1,\ 4,\ 0)=11$. Let us compute the product

$$\widetilde{C}=B\widetilde{A}=(1,2,1,4,0)(1,2,2,5,6)=(1,1,2,6,0)=517>210.$$

We find the alternative set:

$$\widetilde{C}_1=517-\left[\frac{517\cdot2}{2310}\right]\frac{2310}{2}=517>210,$$

$$\widetilde{C}_2=517-\left[\frac{517\cdot3}{2310}\right]\frac{2310}{3}=517>210,$$

$$\widetilde{C}_3=517-\left[\frac{517\cdot5}{2310}\right]\frac{2310}{5}=517-462=55<210,$$

$$\widetilde{C}_4=517-\left[\frac{517\cdot7}{2310}\right]\frac{2310}{7}=517-330=187<210,$$

$$\widetilde{C}_5=517-\left[\frac{517\cdot11}{2310}\right]\frac{2310}{11}=517-420=97<210.$$

Whence

$$\mathfrak{A}(\widetilde{C})=(5,7,11).$$

Page 190.

Consequently,

$$\widetilde{\mathfrak{A}}(\widetilde{C}) = (7, 11)(5, 7, !1) = (7, 11).$$

On the basis of the previous theorem it is possible to exclude from $\widetilde{\mathfrak{A}}(\widetilde{C})$ basis/base $p_5 = 11$. thereby to shear/section we localize unambiguously the error: in A is incorrect digit 5 on basis/base p_4.

Note. Is here carried out multiplication by B on the assumption that it enters into program in accordance with the formulated above agreement.

The otherwise carried out operation and the revealed inaccuracy of digit on basis/base $p_4 = 7$ would not have real sense. Since for the separately undertaken number possibilities of errors on any of the bases/bases, entering the alternative set, are equal, then by any artificially introduced operation cannot be set, what in reality must be a true number. Only the operations of real programs, which satisfies agreement, on which must be treated a true number, can come to light/detect/expose the occurred error by only manner carry out a selection of the necessary correction of all possible for this number

corrections.

Theorem 4.15. let in the regulated system of the bases/bases

$$p_1, \ p_2, \ \ldots, \ p_n, \ p_{n+1}$$

preset the incorrect number

$$\widetilde{A} = (\alpha_1', \ \alpha_2', \ \ldots, \ \alpha_j', \ \ldots, \ \alpha_n', \ \alpha_{n+1}')$$

with alternative totality $\mathfrak{A}(\widetilde{A})$, into which enter basis/base p_j and it
is preset, that in the case of receiving the hypothesis of the
inaccuracy of digit α_j' on basis/base p_j the latter must be corrected
on α_j. Then if during the calculation of certain rational integral
function $f(\widetilde{A})$

$$\widetilde{C} = f(\widetilde{A}) = (\gamma_1', \ \gamma_2', \ \ldots, \ \gamma_j', \ \ldots, \ \gamma_n', \ \gamma_{n+1}'),$$

of such, that

$$\gamma_j' = f(\alpha_j') = f(\alpha_j),$$

we obtain as a result the incorrect number $\widetilde{C}$, then digit α_j' cannot be
erroneous.

Proof. Actually/really, if digit α_j' is erroneous, then correct
is digit α_j. That as during calculation $\widetilde{C}$ digit γ_j is the same, as if
in $\widetilde{A}$ on basis/base p_j there was correct digit α_j, the $\widetilde{C}$ must be a
correct number. Thereby the fop of inaccuracy $\widetilde{C}$ refutes assumption
about the inaccuracy of digit α_j'.

Page 191.

Example. In the system of bases/bases $p_1=2$; $p_2=3$; $p_3=5$; $p_4=7$; $p_5=11$ number $\widetilde{A}=(1, 1, 3, 1, 1) =463>210$ it has alternative set $\mathfrak{A}(\widetilde{A})=(5, 7, 11)$.

Let us compute the alternative set of the number

$$\widetilde{C}=(\widetilde{A})^2+31.$$

Let us compute value

$$\widetilde{C}=(1, 1, 3, 1, 1)\cdot(1, 1, 3, 1, 1)+(1, 1, 1, 3, 9)$$
$$=(0, 2, 0, 4, 10)=1880>211.$$

As it is easy to count, the alternative set of number $\widetilde{C}$ is equal to $\mathfrak{A}(\widetilde{C})=(5, 11)$, whence the conditional alternative set

$$\widetilde{\mathfrak{A}}(\widetilde{C})=(5, 7, 11)(5, 11)=(5, 11).$$

For refinement $\widetilde{\mathfrak{A}}(C)$ we check in accordance with the previous theorem digit on basis/base p_5.

We note that after allowing the presence of error on basis/base 11 we will obtain for the corrected digit value of 10. We compute on corrected digit 10 the appropriate digit $\widetilde{C}$:

$$(10^2+9)(\bmod 11)=10.$$

It coincided with the calculated digit in $\widetilde{C}$ in basis/base p_5. With this $\widetilde{C}$ - incorrect number. Consequently, in $\widetilde{A}$ digit $\alpha_5=1$ on basis/base p_5 correct and basis/base p_5 must be excluded from $\widetilde{\mathfrak{A}}(\widetilde{C})$. We

obtain $\tilde{u}(\tilde{C}) = (5)$, that consisting of one basis/base. It here proved to be possible to completely localize error.

§ 4.6. Logical strengthening of control basis/base.

Above it was established/installed, that surplus basis/base always enters into alternative set how is determined the impossibility of the single-valued contraction of alternative to erroneous basis/base, if short duration failure occurred not on the control basis/base. It is possible only indirectly to judge the inaccuracy of digit by basis/base p_j, when for the elongation/extent relative to the prolonged section of circuit alternative set does not subtend to p_{n+1}, and it remains that containing pair (p_j, p_{n+1}), since, if error affected basis/base p_{n+1}, alternative set must compulsorily be tightened to p_{n+1}. However, similar indirect criteria can require the presence of long circuit for the testing for contraction to p_{n+1} and they cannot completely exclude the cases when conclusion about inaccuracy p_j is not justified.

Page 192.

Therefore it is expedient to consider the formulated previously task of this strengthening of control basis/base, which would make it possible to exclude p_{n+1} from the alternative set as the basis/base

on which the error occur cannot. Clear the technical methods of this strengthening, let us consider the following logical way of the reliable introduction of surplus basis/base.

Above was examined the representation of numbers in operating range $\mathscr{P}$ and full/total/complete $P = p_{n+1}\mathscr{P}.$ Let us now present numbers in operating range P, and as surplus basis/base let us take $p_{n+2} > p_{n+1}.$ In this case full/total/complete range will be number $\tilde{P} = p_{n+2}P.$ However, numbers in the full/total/complete range $\tilde{P}$ we will represent by special form, namely, if this number $A < \tilde{P}$ can be represented in the adopted system from n+2 bases/bases in the form

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_{n+1}, \alpha_{n+2}),$$

then the special machine representation of number A will be the number

$$A - \alpha_{n+2} = (\beta_1, \beta_2, \ldots, \beta_{n+1}, 0),$$

if

$$2\alpha_{n+2} < p_{n+2},$$

or

$$A + p_{n+2} - \alpha_{n+2} = (\beta_1, \beta_2, \ldots, \beta_{n+1}, 0),$$

if

$$2\alpha_{n+2} > p_{n+2}.$$

In other words all machine of a number have a digit 0 on surplus basis/base and the rational operations on machine numbers they must also give zero on this basis/base. Consequently, it is possible not

at all to implement on basis/base p_{n+2} of any operations, but to always consider that the results have zero on this basis/base. Thus, on surplus basis/base is achieved/reached complete reliability, since it directly in the realization cf operations does not participate and true result of operation on this basis/base is previously predetermined. The expansion of operating range from $\mathscr{P}$ to P is substantially necessary for retaining/preserving/maintaining the accuracy of the representation of values in the range $\mathscr{P}$, since by the special representation of a number is built-in the error whose maximum value $\frac{1}{2}(p_{n+2}-1)$.

Page 193.

So that the accuracy of representation would not undergo noticeable decrease, it is necessary to increase the range of the representation of values, and then their true (without the introduced error) values will be in the limits of the preset operating range.

Let us consider an example of the special representation of numbers in the system with bases/bases $p_1=2$; $p_2=3$; $p_3=5$; $p_4=7$; $p_5=11$. Its range is equal to $\mathscr{P}=2\cdot3\cdot5\cdot7\cdot11=2310$. Let us introduce surplus basis/base $p_6=13$.

Let us point out the orthogonal bases of formed in this way

system

$$B_1 = 15 \cdot 015; \quad B_2 = 20 \cdot 020; \quad B_3 = 6 \cdot 006; \quad B_4 = 25 \cdot 740;$$
$$B_5 = 16 \cdot 380; \quad B_6 = 6930.$$

In this case full/total/complete range will be $P = 30 \cdot 030$. It is necessary to present in the special form number $A = 1743$. We find the digits of the representation of a number according to all bases/bases $A = (1, 0, 3, 0, 5, 1)$. Here $\alpha_{n+2} = 1$. Instead of A we take $A - 1 = (0, 2, 2, 6, 4, 0)$, that has digit 0 on basis/base p_6 and exclude this basis/base, we will obtain $A' = (0, 2, 2, 6, 4)$.

In conclusion let us note that during the representation of a number in the special form the form of its alternative set is retained.

§ 4.7. Distribution of isolated errors according to the intervals of operating range.

One of the methods of determining the correctness of the number

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1})$$

is the so-called method of nulling, which consists into the transition from an initial number to the number

$$(0, 0, \ldots, 0, \gamma_{n+1})$$

with the help of such sequence of conversions with which occurs not one departure beyond the operating range of system.

In other words nulling a number consists in the consecutive subtraction from an initial number of some minimum numbers - the constants of nulling such, that number A consistently is converted into a number of form

$$(0, \alpha_2', \alpha_3', \ldots, \alpha_n', \alpha_{n+1}'),$$

then into the number

$$(0, 0, \alpha_3'', \ldots, \alpha_n'', \alpha_{n+1}''),$$

further into a number of form

$$(0, 0, 0, \alpha_4''', \ldots, \alpha_n''', \alpha_{n+1}''').$$

Page 194.

Continuing this process of n of times, we will obtain

$$(0, 0, 0, \ldots, 0, \gamma_{n+1}).$$

In this case the constants of nulling must be selected in such a way that during the subtractions would occur not one departure from the operating range of system.

In other words, if the intermediate result of nulling takes the form

$$(0, 0, \ldots, 0, \alpha_i^{(i-1)}, \alpha_{i+1}^{(i-1)}, \ldots, \alpha_{n+1}^{(i-1)}),$$

then as the next constant of nulling must be selected small from possible numbers of the form

$$(0, 0, \ldots, 0, \alpha_i^{(i-1)}, t_{i+1}, \ldots, t_{n+1}),$$

then during the subtraction is guaranteed the absence of transition

through the range.

Thus, as the constants of nulling are chosen such M of the numbers, which are the smallest possible numbers of form:

$$(t_{1,1}, t_{2,1}, \ldots, t_{n+1,1}), \quad t_{1,1} = 1, 2, \ldots, p_1 - 1;$$
$$(0, t_{2,2}, \ldots, t_{n+1,2}), \quad t_{2,2} = 1, 2, \ldots, p_2 - 1;$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(0, 0, \ldots, 0, t_{n,n}, t_{n+1,n}), \quad t_{n,n} = 1, 2, \ldots, p_n - 1.$$

In this case the total quantity of constants will be defined as

$$\sum_{i=1}^{n} p_i - n.$$

Nulling a number, we consecutively/serially pass from it to the nearest smaller number, multiple p_1, then to a number, multiple $p_1 p_2$ and finally we pass to the nearest smallest number, multiple

$$\mathscr{P} = \prod_{i=1}^{n} p_i.$$

In this case should be noted the fact that the result of nulling does not depend on that, in what sequence (in what order) are nulled the single digits of a number.

Page 195.

Theorem 4.16. If in the regulated system of the bases/bases

$$p_1, p_2, \ldots, p_n, p_{n+1}$$

nulling the number

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}),$$

then the result of the nulling

$$A' = (0, 0, \ldots, 0, \gamma_{n+1})$$

does not depend on that, in which order were nulled the digits of an initial number.

Proof. Let us arbitrarily number first n of the bases/bases

$$p_1, p_2, \ldots, p_n$$

and let us consider the representation of a number in the system where bases/bases $p_i (i = 1, 2, \ldots, n)$ are arranged in the arbitrary order

$$p_{j_1}, p_{j_2}, \ldots, p_{jn}.$$

Each of $j_1, j_2, \ldots, j_n$ here accepts one of the values of 1, 2 ..., n.

Then, regarding, the constants of nulling on first basis/base p_{j_1} will be the numbers

$$1, 2, \ldots, p_{j_1} - 1;$$

on the second basis/base

$$p_{j_1}, 2p_{j_1}, \ldots, (p_{j_2} - 1)p_{j_1};$$
$$\cdots\cdots\cdots\cdots\cdots$$

on j_k -мu to the basis/base

$$\prod_{i=1}^{k-1} p_{j_i}, \ 2\prod_{i=1}^{k-1} p_{j_i}, \ \ldots, \ (p_{j_k} - 1)\prod_{i=1}^{k-1} p_{j_i};$$

and finally on the latter/last basis/base

$$\prod_{i=1}^{n-1} p_{j_i}, \ 2\prod_{i=1}^{n-1} p_{j_i}, \ \ldots, \ (p_{jn} - 1)\prod_{i=1}^{n-1} p_{j_i}.$$

Since in each stage of nulling it is used only by one of the

constants of each level, the great number C, which can be subtracted
in the process of nulling from an initial number, it will be defined
as

$$C = (p_{j_1} - 1) + (p_{j_2} - 1) p_{j_1} - \ldots - (p_{j_n} - 1) \prod_1^{n-1} p_i - \prod_{i=1}^{n} p_i - 1$$

or

$$C = \mathscr{P} - 1.$$

Page 194.

Thus, independent of the order of nulling the great number which is
subtracted from the initial, it is less than the value of operating
range.

Hence in the process of nulling we can swit h over only to one
number, which lies on the left border of that interval $[j\mathscr{P}, (j - 1)\mathscr{P})$,
at which it was located the initial number being nulled.

Corollary 1. The result of nulling determines the number of the
interval, in which there was placed the number being nulled.

Actually/really, since as a result we obtain the number, which
lies on the left border of interval $[j\mathscr{P}, (j + 1)\mathscr{P})$, at which it was
located an initial number, then occurs the equality

$$j\mathscr{P} = \gamma_{n+1} m_{n+1} \pmod{p_{n+1}} \mathscr{P}$$

or

$$j \equiv \gamma_{n+1} m_{n+1} \pmod{p_{n+1}}. \qquad (4.10)$$

Corollary 2. If an initial number was correct, then for it $j = 0$,

whence follows $\gamma_{n+1} \equiv 0 \pmod{p_{n+1}}$, i.e. as a result of nulling a correct number they must obtain the zero number

$$(0, 0, \ldots, 0, 0).$$

Then according to the result of nulling it is possible to judge about correctness of the number: if $\gamma_{n+1} = 0$, the number correct; if $\gamma_{n+1} \neq 0$, the number is incorrect and is arranged/located in interval $[j\mathcal{P}, (j+1)\mathcal{P})$.

Theorem 4.17. (about the error distribution). If in the regulated system of the bases/bases

$$p_1, p_2, \ldots, p_n, p_{n+1}$$

is preset the incorrect number

$$\widetilde{A} = (\alpha_1, \ldots, \alpha_{i-1}, \widetilde{\alpha}_i, \alpha_{i+1}, \ldots, \alpha_n, \alpha_{n+1}).$$

inaccuracy of which is caused by error $\Delta\alpha_i$ in digit α_i on basis/base p_i, i.e.

$$\widetilde{\alpha}_i = \alpha_i + \Delta\alpha_i \pmod{p_i},$$

and if as a result of nulling of number $\widetilde{A}$ we obtain the number

$$(0, 0, \ldots, 0, \gamma_{n+1}),$$

then the number of interval $j+1$, into which falls the incorrect number $\widetilde{A}$, it is limited by the formula

$$j = \left[\frac{\Delta\alpha_i m_i p_{n+1}}{p_i} \right] \pmod{p_{n-1}} - \delta. \qquad (4.11)$$

where δ can take values of 0 or 1.

Page 197.

Proof. The left edge of interval $[j\mathcal{P}, (j+1)\mathcal{P})$ is determined from the relationship/ratio

$$j = \frac{\dfrac{P}{p_{n+1}} m_{n+1} \gamma_{n+1} - kP}{\dfrac{P}{p_{n+1}}} = m_{i-1} \gamma_{i-1} \pmod{p_{i-1}}.$$

where k - whole non-negative number.

In accordance with theorem condition we occur the equality

$$\widetilde{A} = A + (0, 0, \ldots, 0, \Delta\alpha_i, 0, \ldots, 0),$$

where A - is the correct number:

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n, \alpha_{n+1}).$$

In other words addition to the correct number A of the number

$$(0, 0, \ldots, \Delta\alpha_i, \ldots, 0)$$

shifts result from the first interval into the interval with number j+1 or j+2, i.e.,

$$j - \delta = \left[\frac{\Delta\alpha_i m_i \dfrac{P}{p_i}}{\dfrac{P}{p_{n+1}}} \right] \pmod{p_{n+1}} = \left[\frac{\Delta\alpha_i m_i p_{n+1}}{p_i} \right] \pmod{p_{n+1}}.$$

whence follows assertion (4.11) of theorem.

Corollary. For the standardized/normalized regulated system expression (4.11) of theorem.

$$j = \gamma_{n+1} = \left[\frac{\Delta\alpha_i m_i p_{n+1}}{p_i} \right] \pmod{p_{n+1}} - \delta. \qquad (4.12)$$

Theorem 4.18. (about the error distribution).

Page 198.

If in the regulated system of the bases/bases

$$p_1, p_2, \ldots, p_n, p_{n+1}$$

is preset the incorrect number

$$\widetilde{A} = (\alpha_1, \ldots, \alpha_{i-1}, \widetilde{\alpha}_i, \alpha_{i+1}, \ldots, \alpha_{n+1}),$$

inaccuracy of which is caused by error $\Delta\alpha_i$ in digit $\widetilde{\alpha}_i$ on basis/base p_i, i.e.

$$\widetilde{\alpha}_i = \alpha_i \dotplus \Delta\alpha_i \,(\mathrm{mod}\,p_i),$$
$$\Delta\alpha_i = 1, 2, \ldots, p_i - 1,$$

where α_i - digit on basis/base p_i of the correct number

$$A = (\alpha_1, \ldots, \alpha_{i-1}, \alpha_i, \alpha_{i+1}, \ldots, \alpha_{n+1}),$$

and if the result of nulling the number

$$(0, 0 \ldots 0, \Delta\alpha_i, 0 \ldots 0, 0)$$

takes the form

$$(0, 0, \ldots, 0, \gamma_{n+1}),$$

then the value of error $\Delta\alpha_i$ is determined by the equality

$$\Delta\alpha_i = \left(\frac{p_{n+1} - \gamma_{n+1}}{c_{n+1}} \,(\mathrm{mod}\,p_{n+1})\, c_i \right) (\mathrm{mod}\,p_i), \qquad (4.13)$$

where c_i and c_{n+1} are the digits of the number

$$\frac{\mathcal{P}}{p_i} = (0, 0, \ldots, 0, c_i, 0, \ldots, 0, c_{n+1}).$$

Proof. Since the result of nulling does not depend on the order of nulling, then, carrying out the process indicated on numbers A and $\tilde{A}$ through the digits of the bases/bases

$$p_1, p_2, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n,$$

we will obtain the numbers

$$(0, 0, \ldots, 0, \tilde{\beta}_i, 0, \ldots, 0, \beta_{n+1}) \qquad (4.14)$$

and

$$(0, 0, \ldots, 0, \beta_i, 0, \ldots, 0, \beta_{n+1}) \qquad (4.15)$$

respectively.

The completion of the process of nulling must be produced by the constants of the form

$$\frac{\mathscr{P}}{p_i} ; \ 2\frac{\mathscr{F}}{p_i} ; \ \ldots; (p_i - 1)\frac{\mathscr{P}}{p_i} .$$

Let us select pair λ_i and λ_i' of such whole non-negative numbers that would be satisfied the condition

$$\lambda_i' c_i = \tilde{\beta}_i \,(\mathrm{mod}\, p_i), \qquad (4.16)$$
$$\lambda_i c_i = \beta_i \,(\mathrm{mod}\, p_i). \qquad (4.17)$$

Page 199.

Multiplying λ_i' and λ_i on $\frac{\mathscr{P}}{p_i}$ and subtracting respectively from (4.14) and (4.15) we will obtain

$$\beta_{n+1} - \lambda_i' c_{n+1} = \gamma_{n+1} \,(\mathrm{mod}\, p_{n+1}),$$
$$\beta_{n+1} - \lambda_i c_{n+1} = 0 \,(\mathrm{mod}\, p_{n+1}),$$

whence

$$\lambda_i' - \lambda_i = \frac{p_{n+1} - \gamma_{n+1}}{c_{n+1}} \,(\bmod\, p_{n+1}), \qquad (4.18)$$

where the division it is understood as formal division on modulus/module p_{n+1}.

From (4.16) and (4.17) we will obtain

$$(\lambda_i' - \lambda_i)\, c_i = (\widetilde{\beta}_i - \beta_i)\,(\bmod\, p_i). \qquad (4.19)$$

On the strength of the fact that expressions (4.14) and (4.15) are obtained as a result of identical process, we have

$$\widetilde{\beta}_i - \beta_i = \Delta\alpha_i,$$

i.e.

$$(\lambda_i' - \lambda_i)\, c_i = \Delta\alpha_i \,(\bmod\, p_i),$$

whence and follows the assertion of theorem.

Since each of the errors can translate a correct number into the number, which lies only at one of two intervals

$$[j\mathscr{P},\ (j+1)\mathscr{P}),\ [(j+1)\mathscr{P},\ (j+2)\mathscr{P}),$$

then, knowing the number of interval, where hit an incorrect number, can be defined as the set of bases/bases, in the digits on which could take place the error, so also possible value of error, which translates correct number into this interval.

In connection with this are opened further possibilities to the reduction of the process of position finding of error, namely:

- since the error in the digits from bases/bases p_1, p_2, ...,
p_n can be available only in intervals determined by theorem 4.17,
then in the case when occurs the error, which relates not to one and
possible intervals, it is possible to claim that it occurred in the
digit on control base;

- since the rum of the information about the possible location
of error we possess the information also about the value of the
predicted error, then this further information in a number of cases
will make it possible to more rapidly determine true value and
location of error;

- in the case when the alternative set of bases/bases subtends
to one basis/base, to us is immediately known the value to which
should be corrected the digit on this basis/base.

Page 200.

Let us consider the distribution of incorrect numbers according
to the intervals of numerical range for the concrete/specific/actual
system of bases/bases $p_1=2$; $p_2=3$; $p_3=5$; $p_4=7$; $p_5=11$. Let us give the
values of minimum numbers of nulling in this system

(1, 1, 1, 1, 1)	(0, 0, 2, 5, 1)	(0, 0, 0, 2, 8)
(0, 1, 4, 4, 4)	(0, 0, 3, 4, 7)	(0, 0, 0, 3, 7)
(0, 2, 2, 2, 2)	(0, 0, 4, 3, 2)	(0, 0, 0, 4, 5)
(0, 0, 1, 6, 6)	(0, 0, 0, 1, 10)	(0, 0, 0, 5, 4)
		(0, 0, 0, 6, 2)

Let us consider the distribution of incorrect numbers according to the intervals of numerical range depending on the value of error.

Basis/base $p_1 = 2$.

For a number with the error $\Delta \alpha_1 = 1$

$$\gamma_5 = \left[\frac{11}{2} \right] (\text{mod } 11) + \delta = 5 + \delta,$$

i.e. the error translates numerical into the sixth or seventh interval.

Basis/base $p_2 = 3$.

For error $\Delta \alpha_2 = 1$

$$\gamma_5 = \left[\frac{2 \cdot 11}{3} \right] (\text{mod } 11) + \delta = 7 + \delta.$$

A number will pass into the eighth or ninth intervals.

Error $\Delta \alpha_2 = 2$ gives

$$\gamma_5 = \left[\frac{4 \cdot 11}{3} \right] (\text{mod } 11) + \delta = 3 + \delta$$

and will translate a number into the fourth or fifth intervals.

Basis/base $p_3 = 5$.

For the error $\Delta \alpha_3 = 1$ we will obtain

$$\gamma_5 = \left[\frac{3 \cdot 11}{5}\right] (\bmod 11) + \delta = 6 + \delta.$$

With the error $\Delta \alpha_3 = 2$ we will obtain

$$\gamma_5 = \left[\frac{2 \cdot 3 \cdot 11}{5}\right] (\bmod 11) + \delta = 2 + \delta.$$

Page 201.

With $\Delta \alpha_3 = 3$ we will obtain

$$\gamma_5 = \left[\frac{3 \cdot 3 \cdot 11}{5}\right] (\bmod 11) + \delta = 8 + \delta.$$

With $\Delta \alpha_3 = 4$ we will have

$$\gamma_5 = \left[\frac{4 \cdot 3 \cdot 11}{5}\right] (\bmod 11) + \delta = 4 + \delta.$$

Basis/base $p_4 = 7$.

A number with the error $\Delta \alpha_4 = 1$ will give

$$\gamma_5 = \left[\frac{11}{7}\right] (\bmod 11) + \delta = 1 + \delta.$$

Error $\Delta \alpha_4 = 2$ translates a number into the interval, determined

$$\gamma_5 = \left[\frac{2 \cdot 11}{7}\right] (\bmod 11) + \delta = 3 + \delta.$$

$\Delta \alpha_4 = 3$ is translated a number into the interval, which corresponds

$$\gamma_5 = \left[\frac{3 \cdot 11}{7}\right] (\bmod 11) + \delta = 4 + \delta.$$

With $\Delta \alpha_4 = 4$ we will obtain

$$\gamma_5 = \left[\frac{4 \cdot 11}{7}\right] (\bmod 11) + \delta = 6 + \delta.$$

With $\Delta \alpha_4 = 5$ we will have

$$\gamma_5 = \left[\frac{5 \cdot 11}{7}\right] (\bmod 11) + \delta = 7 + \delta.$$

Error $\Delta\alpha_4=6$ will translate a number into the interval, determined

$$\gamma_5 = \left[\frac{6 \cdot 11}{7}\right] \pmod{11} + \delta = 9 \div \delta.$$

The obtained results make it possible to construct the table, in which to values γ_5 are compared possible errors $\Delta\alpha_i$. It is doubtless so that to each value γ_5 can correspond error, also, on the control basis/base. After designating it through Δ_k, we will have as the possible error a value $\Delta_k = \gamma_5$ (see tables on page 202).

Example. Let be is preset the incorrect number $\widetilde{A} = (1, 1, 4, 1, 1)$, to which in resolving task is adjoined the correct number $B = (0, 2, 0, 4, 2)$. Let us try to determine location and value of error in number $\widetilde{A}$.

Let us lead nulling number $\widetilde{A}$

$$
\begin{array}{ccc}
(1, 1, 4, 1, 1) & (0, 0, 3, 0, 0) & (0, 0, 0, 3, 4) \\
-(1, 1, 1, 1, 1) & -(0, 0, 3, 4, 7) & -(0, 0, 0, 3, 7) \\
\hline
(0, 0, 3, 0, 0) & (0, 0, 0, 3, 4) & (0, 0, 0, 0, 8)
\end{array}
$$

Page 202.

Since $\gamma_5 = 8$, then from the given table let us determine the following alternative set:

- or occurs the error $\Delta\alpha_2 = 1$ in the digit on basis/base p_2;

- or occurs the error $\Delta\alpha_3 = 3$ in the digit on basis/base p_3;

- or occurs the error $\Delta\alpha_4=5$ in the digit on basis/base p_4;

or occurs error $\Delta_k=8$ in the digit on the control basis/base.

Let us fulfill the operation of adding of number $\widetilde{A}$ with number B

$$\widetilde{A} + B = (1, 1, 4, 1, 1) + (0, 2, 0, 4, 2) = (1, 0, 4, 5, 3).$$

The table of error distribution.

(1) Значение Y_5	(2) Возможные ошибки
0	(3) Число правильное, ошибок нет
1	$\Delta\alpha_4 = 1, \quad \Delta_h = 1$
2	$\Delta\alpha_3 = 2, \quad \Delta\alpha_4 = 1, \quad \Delta_h = 2$
3	$\Delta\alpha_2 = 2, \quad \Delta\alpha_3 = 2, \quad \Delta\alpha_4 = 2, \quad \Delta_h = 3$
4	$\Delta\alpha_2 = 2, \quad \Delta\alpha_3 = 4, \quad \Delta\alpha_4 = 2, \quad \Delta\alpha_4 = 3, \quad \Delta_h = 4$
5	$\Delta\alpha_1 = 1, \quad \Delta\alpha_3 = 4, \quad \Delta\alpha_4 = 3, \quad \Delta_h = 5$
6	$\Delta\alpha_1 = 1, \quad \Delta\alpha_3 = 1, \quad \Delta\alpha_4 = 4, \quad \Delta_h = 6$
7	$\Delta\alpha_2 = 1, \quad \Delta\alpha_3 = 1, \quad \Delta\alpha_4 = 4, \quad \Delta\alpha_4 = 5, \quad \Delta_h = 7$
8	$\Delta\alpha_2 = 1, \quad \Delta\alpha_3 = 3, \quad \Delta\alpha_4 = 5, \quad \Delta_h = 8$
9	$\Delta\alpha_3 = 3, \quad \Delta\alpha_4 = 6, \quad \Delta_h = 9$
10	$\Delta\alpha_4 = 6, \quad \Delta_h = 10$

Key: (1). Value. (2). Possible errors. (3). Number correct, there are no errors.

Page 203.

    Nulling the obtained sum

$$
\begin{array}{ll}
(1, 0, 4, 5, 3) & (0, 2, 3, 4, 2) \\
-(1, 1, 1, 1, 1) & -(0, 2, 2, 2, 2) \\
\hline
(0, 2, 3, 4, 2) & (0, 0, 1, 2, 0) \\
(0, 0, 1, 2, 0) & (0, 0, 0, 3, 5) \\
-(0, 0, 1, 6, 6) & -(0, 0, 0, 3, 7) \\
\hline
(0, 0, 0, 3, 5) & (0, 0, 0, 0, 9)
\end{array}
$$

For the sum obtained $\gamma_5 = 9$ and in accordance with the table of error distribution let us determine the possible alternative set:

- either occurs error $\Delta\alpha_3 = 3$ on basis/base p_3,

- or occurs error $\Delta\alpha_4 = 6$ on basis/base p_4,

- or occurs error $\Delta_k = 9$ on the control basis/base.

Since neither value nor location of error could be changed, then it is possible to claim that occurs the error $\Delta\alpha_3 = 3$ on basis/base p_3.

Hence unknown corrected number A can be represented as

$$A = \tilde{A} - (0, 0, 3, 0, 0) = (1, 1, 1, 1, 1).$$

The example examined demonstrates the fact that an increase in the informativeness of alternative set allowed for one step/pitch not only to determine the location of error, but also to indicate its value.

It should be noted that the error distribution according to the intervals of numerical range as the rate of convergence of the alternative set of errors, depends on the value of control basis/base, i.e., from that occurring for redundancy.

Theorem 4.19 (maximum). If in the standardized/normalized regulated system occurs the relationship/ratio

$$p_{n+1} > 2p_n p_{n-1}, \qquad (4.20)$$

Then the number of interval $[j\mathscr{P}, (j+1)\mathscr{P})$, into which falls the number, which contains error on one of the working bases/bases, are uniquely determined location and value of error.

Proof. On the basis of theorem 4.17 about the error distribution the number of interval $j+1$, where falls number $\widetilde{A}$ in the presence of error $\Delta\alpha_i$ it is defined as

$$j = \left[\frac{\Delta\alpha_i m_i p_{n+1}}{p_i} \right] (\bmod\ p_{n+1}) \div \delta,$$

i.e. a number it falls either into the interval with the number

$$\left[\frac{\Delta\alpha_i m_i p_{n+1}}{p_i} \right] (\bmod\ p_{n+1}).$$

or

$$\left[\frac{\Delta\alpha_i m_i p_{n+1}}{p_i} \right] (\bmod\ p_{n+1}) + 1.$$

Page 204.

The condition of the fact that into the intervals with such numbers cannot hit an incorrect number, as a result of the appearance of an

error on any of the working bases/bases p_j it will be

$$\left| \left[\frac{\Delta \alpha_i m_i p_{n+1}}{p_i} \right] - \left[\frac{\Delta \alpha_j m_j p_{n+1}}{p_j} \right] \right| (\mathrm{mod}\, p_{n+1}) \geqslant 2$$

or, after amplifying inequality,

$$\left[\left| \frac{\Delta \alpha_i m_i p_j p_{n+1}}{p_i p_j} - \frac{\Delta \alpha_j m_j p_i p_{n+1}}{p_i p_j} \right| \right] (\mathrm{mod}\, p_{n+1}) > 2,$$

whence

$$\left[\frac{p_{n+1}}{p_i p_j} \left| \Delta \alpha_i m_i p_j - \Delta \alpha_j m_j p_i \right| \right] (\mathrm{mod}\, p_{n+1}) > 2. \quad (4.21)$$

Value

$$\left| \Delta \alpha_i m_i p_j - \Delta \alpha_j m_j p_i \right| \neq 0$$

is positive integer number. Hence with

$$p_{n+1} > 2 p_n p_{n-1}$$

is satisfied the condition (4.21) that also is claimed in the theorem.

Let us consider the operation of theorem in the concrete/specific/actual system of the bases/bases

$$p_1 = 3; \quad p_2 = 5; \quad p_3 = 7.$$

Let us select the control basis/base $p_4 = 71 > 2 p_2 p_3.$

In this case the docking range $\mathscr{P} = 105$, and the complete range $P = 7455$. Orthogonal bases with their weights will be determined

$$B_1 = 2485, \ m_1 = 1, \ B_2 = 1491, \ m_2 = 1, \ B_3 = 1065,$$
$$m_3 = 1, \ B_4 = 2415, \ m_4 = 23.$$

Let us write out minimum numbers of nulling:

on basis/base $p_1 = 3$

$$(1, 1, 1, 1)$$
$$(2, 2, 2, 2)$$

on basis/base $p_2 = 5$

$$(0, 1, 6, 6)$$
$$(0, 2, 5, 12)$$
$$(0, 3, 3, 3)$$
$$(0, 4, 2, 9)$$

on basis/base $p_3=7$

$$(0, 0, 1, 15)$$
$$(0, 0, 2, 30)$$
$$(0, 0, 3, 45)$$
$$(0, 0, 4, 60)$$
$$(0, 0, 5, 4)$$
$$(0, 0, 6, 19)$$

Page 205.

Let us consider error distribution according to the intervals of basis/base $p_1=3$.

Error $\Delta\alpha_1=1$. Let us null number $(1, 0, 0, 0)$

$(1, 0, 0, 0)$	$(0, 4, 6, 70)$	$(0, 0, 1, 61)$
$-(1, 1, 1, 1)$	$-(0, 4, 2, 9)$	$-(0, 0, 4, 60)$
$(0, 4, 6, 70)$	$(0, 0, 4, 61)$	$(0, 0, 0, 1)$

Since $\gamma_4=1$, then the number of interval N will be defined as $N=1\cdot23$ (mod 71)$+1=24$.

Error $\Delta\alpha_1=2$. Let us null number $(2, 0, 0, 0)$

$(2, 0, 0, 0)$	$(0, 3, 5, 69)$	$(0, 0, 2, 66)$
$-(2, 2, 2, 2)$	$-(0, 3, 3, 3)$	$-(0, 0, 2, 30)$
$(0, 3, 5, 69)$	$(0, 0, 2, 66)$	$(0, 0, 0, 36)$

Hence $N=36\cdot23$ (mod 71)$+1=48$.

On basis/base $p_2=5$ $\Delta\alpha_2=1$. Let us null $(0, 1, 0, 0)$

$$(0, 1, 0, 0) \qquad (0, 0, 1, 65)$$
$$\underline{-(0, 1, 6, 6)} \qquad \underline{-(0, 0, 1, 15)}$$
$$(0, 0, 1, 65) \qquad (0, 0, 0, 50)$$

Here $N=50 \cdot 23$ (mod 71) $+1=15$.

$\Delta\alpha_2=2$. Erroneous number $(0, 2, 0, 0)$

$$(0, 2, 0, 0) \qquad (0, 0, 2, 59)$$
$$\underline{-(0, 2, 5, 12)} \qquad \underline{-(0, 0, 2, 70)}$$
$$(0, 0, 2, 59) \qquad (0, 0, 0, 29)$$

Whence $N=29 \cdot 23$ (mod 71) $+1=29$.

$\Delta\alpha_2=3$. Let us null number $(0, 3, 0, 0)$

$$(0, 3, 0, 0) \qquad (0, 0, 4, 68)$$
$$\underline{-(0, 3, 3, 3)} \qquad \underline{-(0, 0, 4, 60)}$$
$$(0, 0, 4, 68) \qquad (0, 0, 0, 31)$$

Then $N=8 \cdot 23$ (mod 71) $+1=43$.

$\Delta\alpha_2=4$. Let us null number $(0, 4, 0, 0)$

$$(0, 4, 0, 0) \qquad (0, 0, 5, 62)$$
$$\underline{-(0, 4, 2, 9)} \qquad \underline{-(0, 0, 5, 4)}$$
$$(0, 0, 5, 62) \qquad (0, 0, 0, 58)$$

Whence $N=58 \cdot 23$ (mod 71) $+1=57$.

Page 206.

On basis/base $p_3=7$

$\Delta \alpha_3 = 1$. Let us null number $(0, 0, 1, 0)$

$$
\begin{array}{r}
(0, 0, 1, 0) \\
- (0, 0, 1, 15) \\
\hline
(0, 0, 0, 56)
\end{array}
$$

Then $N = 56 \cdot 23 \pmod{71} + 1 = 11$.

$\Delta x_3 = 2$. Number $(0, 0, 2, 0)$

$$
\begin{array}{r}
(0, 0, 2, 0) \\
- (0, 0, 2, 30) \\
\hline
(0, 0, 0, 41)
\end{array}
$$

Whence $N = 41 \cdot 23 \pmod{71} + 1 = 21$.

$\Delta x_3 = 3$. Let us null $(0, 0, 3, 0)$,

$$
\begin{array}{r}
(0, 0, 3, 0) \\
- (0, 0, 3, 45) \\
\hline
(0, 0, 0, 26)
\end{array}
$$

Whence $N = 26 \cdot 23 \pmod{71} + 1 = 31$.

$\Delta \alpha_3 = 4$. Let us null number $(0, 0, 4, 0)$

$$
\begin{array}{r}
(0, 0, 4, 0) \\
- (0, 0, 4, 60) \\
\hline
(0, 0, 0, 11)
\end{array}
$$

Then $N = 11 \cdot 23 \pmod{71} + 1 = 41$.

$\Delta x_3 = 5$. Number $(0, 0, 5, 0)$

$$
\begin{array}{r}
(0, 0, 5, 0) \\
- (0, 0, 5, 4) \\
\hline
(0, 0, 0, 67)
\end{array}
$$

Whence N=67•23 (mod 71)+1=51.

    $\Delta\alpha_3$=6. Erroneous number (0, 0, 6, 0)

$$\begin{array}{r} (0,\ 0,\ 6,\ 0) \\ -\ (0,\ 0,\ 6,\ 19) \\ \hline (0,\ 0,\ 0,\ 52) \end{array}$$

Whence N=52•23 (mod 71)+1=61.

Thus, an example illustrates the established/installed by limit theorem error distribution according to the intervals of numerical range.

§ 4.8. Arithmetic of errors.

Let us consider some methods of accelerating the contraction of the alternative set of errors with the execution of arithmetic operations.

Theorem 4.20. (About addition and subtraction of errors). If in the regulated system of bases/bases was implemented the correct operation of addition or subtraction whose result was arranged/located in interval γ_r as a result of the appearance of isolated error in one of the operands, then from the alternative set

of errors must be excluded the terms, which dc not satisfy the relationship/ratio

$$|\gamma_\Sigma - \gamma_{\widetilde{A}}| \leqslant 1, \qquad (4.22)$$

where $\gamma_{\widetilde{A}}$ - number of the interval in which was arranged/located incorrect operand.

Page 207.

Proof. By an incorrect number of stood operand $\widetilde{A}$. With the addition (subtraction) to it the correct number B neither value nor location of error be changed can, i.e., the same error occurs also as a result of operation.

Since the number of the interval in which is located the result, is determined by the value of error, and the value of a number itself can move it only into the adjacent interval according to theorem 4.17 about the error distribution, then hence and follows the assertion of theorem.

Theorem 4.21. (About the multiplication of errors). Let in the regulated system of bases/bases be implemented the correct operation of multiplication above operands $\widetilde{A}$ and B whose result C was arranged/located in interval γ_C, as a result of the appearance of isolated error in one of the operands.

Then from the alternative set of errors must be excluded the terms, which do not satisfy the equality

$$\Delta\alpha_i\beta_i(\mathrm{mod}\,p_i) = \Delta c_i, \qquad (4.23)$$

where $\Delta\alpha_i$ - possible error in the digit on basis/base p_i of incorrect operand; β_i - digit on the same basis/base in the correct operand; Δc_i - possible error in the digit of result on the same basis/base.

Proof. For the operation of multiplication we have

$$\alpha_i\beta_i(\mathrm{mod}\,p_i) = c_i. \qquad (4.24)$$

Let us assume that in operand $\widetilde{A}$ on basis/base p_i occurs the error by value $\Delta\alpha_i$, and in the product - by value Δc_i. Then (4.24) it can be rewritten in the form

$$((\alpha_i - \Delta\alpha_i) + \Delta\alpha_i)\,\beta_i(\mathrm{mod}\,p_i) = (c_i - \Delta c_i) + \Delta c_i. \quad (4.25)$$

But if occurs error $\Delta\alpha_i$, the true value $\alpha_i^{(H)}$ of the digit of operand $\widetilde{A}$ on basis/base p_i they are

$$\alpha_i^{(H)} = \alpha_i - \Delta\alpha_i,$$

but the true value of the digit of result $c_i^{(H)}$:

(1) $c_i^{(H)} = c_i - \Delta c_i,$

т. е. $\alpha_i^{(H)}\beta_i(\mathrm{mod}\,p_i) = c_i^{(H)}.$ $\qquad (4.26)$

Key: (1). i.e.

Page 208.

From (4.25) and (4.26) we obtain (4.23).

Theorem 4.22 (About the step-by-step division of errors). Let in the regulated system of bases/bases be implemented the correct operation of the step-by-step division above operands $\widetilde{A}$ and B whose result C as a result of the appearance of isolated error in operand $\widetilde{A}$ became an incorrect number.

Then from the alternative set of errors must be excluded the terms, for which is not implemented the equality

$$\frac{\Delta\alpha_i}{\beta_i}(\bmod p_i) = \Delta c_i, \qquad (4.27)$$

if $\widetilde{A}$ - dividend, or are excluded the terms for which does not occur the equality

$$(\Delta\alpha_i c_i^{(H)} + \Delta c_i \alpha_i^{(H)} + \Delta\alpha_i \Delta c_i)(\bmod p_i) = 0, \qquad (4.28)$$

if the incorrect operand $\widetilde{A}$ is divider/denominator.

Proof. Since is produced the operation of step-by-step division, then takes the place

$$\frac{\alpha_i}{\beta_i}(\bmod p_i) = c_i$$

or

$$\alpha_i + k_i p_i = \beta_i c_i, \qquad (4.29)$$

where k_i - whole non-negative number.

If error on basis/base p_i occurs, then by the true digit of

operand $\widetilde{A}$ on basis/base p_i it will be

$$\alpha_i^{(\text{и})} = \alpha_i - \Delta\alpha_i,$$

but the true digit of the result

$$c_i^{(\text{и})} = c_i - \Delta c_i,$$

whence

$$\alpha_i^{(\text{и})} + k_2 p_i = \beta_i c_i^{(\text{и})}, \qquad (4.30)$$

where k_2 - whole non-negative number. From (4.29) and (4.30) we will

obtain

$$\Delta\alpha_i + k_3 p_i = \beta_i \Delta c_i,$$

where $k_3 = k_1 - k_2$.

Page 209.

Hence

$$\frac{\Delta\alpha_i}{\beta_i}(\text{mod } p_i) = \Delta c_i,$$

that also proves assertion (4.27) of theorem.

In the case, when the incorrect operand $\widetilde{A}$ is

divider/denominator, the execution of step-by-step division can be

registered as

$$\overset{\shortmid\shortmid}{\beta_i} + k_4 p_i = (\alpha_i^{(\text{и})} + \Delta\alpha_i)(c_i^{(\text{и})} + \Delta c_i), \qquad (4.31)$$

where k_4 - whole non-negative number.

But true operation must be implemented above the correct digits

on basis/base p_i, i.e. must occur the relationship/ratio

$$\beta_i + k_5 p_i = \alpha_i^{(\text{и})} c_i^{(\text{и})},\qquad (4.32)$$

where k_5 - whole non-negative number.

From (4.31) and (4.32) we obtain

$$\alpha_i^{(\text{и})}\Delta c_i + c_i^{(\text{и})}\Delta\alpha_i + \Delta\alpha_i\Delta c_i = (k_1 - k_2)\,p_i,$$

whence ensues assertion (4.28) of theorem.

Let us consider the operation of theorems 4.21, 4.22 in the standardized/normalized system of the bases/bases

$$p_1 = 2;\ p_2 = 3;\ p_3 = 5;\ p_4 = 7;\ p_5 = 11.$$

Example. Is preset the incorrect number $\widetilde{A} = (1, 1, 3, 1, 2)$, to which in resolving task correctly is multiplied the correct number $B = (1, 0, 0, 1, 4)$. It is necessary to determine location and value of error.

Nulling the number $\widetilde{A}$

$$
\begin{array}{ll}
(1, 1, 3, 1, 2) & (0, 0, 2, 0, 1) \\
\underline{-(1, 1, 1, 1, 1)} & \underline{-(0, 0, 2, 5, 1)} \\
(0, 0, 2, 0, 1) & (0, 0, 0, 2, 0)
\end{array}
$$

$$
\begin{array}{l}
(0, 0, 0, 2, 0) \\
\underline{-(0, 0, 0, 2, 8)} \\
(0, 0, 0, 0, 3)
\end{array}
$$

They obtained $\gamma_5 = 3$.

Let us null product $\widetilde{A}B$:

$$\widetilde{AB} = (1, 1, 3, 1, 2) \times (1, 0, 0, 1, 4) = (1, 0, 0, 1, 8)$$

(1, 0, 0, 1, 8)	(0, 2, 4, 0, 7)	(0, 0, 2, 5, 5)
(0, 1, 1, 1, 1)	−(0, 2, 2, 2, 2)	−(0, 0, 2, 5, 1)
(0, 2, 4, 0, 7)	(0, 0, 2, 5, 5)	(0, 0, 0, 0, 4)

Here $\gamma_5 = 4$.

Page 210.

From the table of error distribution let us write out the conditional alternative set (p_2, p_3, p_4, p_5).

It is checked now fulfilling of requiring (4.23) the theorem about the multiplication of errors.

Basis/base p_2. We have $\Delta\alpha_2 = 2$, $\beta_2 = 0$, $\Delta c_2 = 2$, i.e., $2 \cdot 0 \neq 2$. Condition (4.23) is not satisfied, the error $\Delta\alpha_2 = 2$ in operand $\widetilde{A}$ is impossible.

Basis/base p_3. We have $\Delta\alpha_3 = 2$, $\beta_3 = 0$, $\Delta c_3 = 4$. Here $2 \cdot 0 \neq 4$, i.e., error $\Delta\alpha_3 = 2$ is impossible and must be excluded from the alternative set.

Basis/base p_4.

a) $\Delta\alpha_4 = 2$, $\beta_4 = 1$, $\Delta c_4 = 2$.   . Here $2 \cdot 1 = 2$. The condition (4.23) is satisfied, error $\Delta\alpha_4 = 2$ is possible.

a) $\Delta\alpha_4 = 2$, $\beta_4 = 1$, $\Delta c_4 = 3$, the condition of theorem $2 \cdot 1 \neq 3$ is not

satisfied. A similar error is impossible.

For control of base $\Delta_k=3$, $\beta_k=4$. $\Delta_c=4$. but $(3 \cdot 4)(\bmod 11) \neq 4$. Error on the control basis/base is impossible.

Thus, error is located in the digit through basis/base p_4 and its value $\Delta\alpha_4=2$.

Example. To determine the alternative set of errors with the execution of the correct operation of dividing the number $\widetilde{A}=(0, 2, 4, 2, 5)$ into the correct number $B=(1, 2, 2, 3, 6)$.

Let us determine the alternative set of the errors for number $\widetilde{A}$, for which let us lead nulling.

$$
\begin{array}{ccc}
(0, 2, 4, 2, 5) & (0, 0, 2, 0, 3) & (0, 0, 0, 2, 2) \\
-(0, 2, 2, 2, 2) & -(0, 0, 2, 5, 1) & -(0, 0, 0, 2, 8) \\
\hline
(0, 0, 2, 0, 3) & (0, 0, 0, 2, 2) & (0, 0, 0, 0, 5)
\end{array}
$$

By value $\gamma_s=5$ from the table we determine the alternative set of errors $(p_1: p_3: p_4: p_5)$, moreover are possible the following values of errors:

$$\Delta\alpha_1=1, \quad \Delta\alpha_3=4, \quad \Delta\alpha_4=3, \quad \Delta_k=5.$$

Let us fulfill the operation of the step-by-step division $\widetilde{A}$ into $B:\widetilde{A}:B=(0, 2, 4, 2, 5):(1, 2, 2, 3, 6)=(0, 1, 2, 3, 10)$.

Let us null the quotient

$$
\begin{array}{cc}
(0, 1, 2, 3, 10) & (0, 0, 3, 6, 6) \\
-(0, 1, 4, 4, 4) & -(0, 0, 3, 4, 7) \\
\hline
(0, 0, 3, 6, 6) & (0, 0, 0, 2, 10)
\end{array}
$$

$$
\begin{array}{c}
(0, 0, 0, 2, 10) \\
-(0, 0, 0, 2, 8) \\
\hline
(0, 0, 0, 0, 2)
\end{array}
$$

By value $\gamma_5 = 2$ we determine for the quotient the alternative set of errors $(p_3; p_4; p_5)$.

In this case conditional alternative set will be

$$
(p_1; p_3; p_4; p_5)(p_3; p_4; p_5) = (p_3; p_4; p_5).
$$

We analyze the obtained set.

Page 211.

Basis/base p_3. $\Delta\alpha_3 = 4$, $\beta_3 = 2$, $\Delta c_3 = 2$. Condition (4.27) $4/2 = 2$ is satisfied, and in the digit on basis/base p_3 is possible error.

Basis/base p_4. $\Delta\alpha_4 = 3$, $\beta_4 = 3$, $\Delta c_4 = 1$. Here $3/5 = 1$. Condition (4.27) is satisfied ~~and~~ and in digit on basis/base p_4 is possible error.

Control basis/base. $\Delta\alpha_5 = 5$, $\beta_5 = 6$, $\Delta c_5 = 2$. According to the condition of the theorem

$$
\frac{5}{6}(\bmod 11) = 10 \neq 2,
$$

i.e. control basis/base must be excluded from the conditional

alternative set. Conditional alternative set will take in this case
form (p_3, p_4).

Knowledge of location and the value of possible error permits
for us to sufficiently efficiently reduce the value of the
conditional alternative set of the errors and in the majority of the
cases to immediately correct place error.

§ 4.9. The statistical simulation of the process of the convergence
of alternative correction.

The simulation of the retraction of alternative sets was
produced to to block diagram on page 212.

As the basis of the system of numeration were selected the
following:
$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \quad p_5 = 11,$$
$$p_6 = 13, \quad p_7 = 29, \quad p_8 = 31, \quad p_9 = 37, \quad p_{10} = 41.$$

In numbers both initial and for the intermediate operations they
were chosen randomly from operating range $\left[0, \dfrac{\overline{P}}{p_{n+1}}\right)$ so that the results
of operation, entering the circuit, would not exceed the limits of
the same range. Furthermore, in the program of the circuit of
operations participated the operations, which substantially vary
value and character of a number. It is completely logical that such
operations, as addition + 1, little varying value numbers, do not

affect the character of the alternative set of a number and thereby do not obtain new information for position finding errors. Therefore poorly informative operations were not built-in into the program of circuit.

Were traced two models of the short duration failures:

1. Always goes out of order one and the same basis/base (and so on each of the bases/bases).

Page 212.

(1) Выбор исходного числа А

(2) Выбор номера основания с искаженной цифрой

(3) Получение искаженного числа А

(4) Нахождение альтернативной совокупности А

(5) Нахождение пересечения альтернативных совокупностей

(6) Анализ окончания процесса стягивания

(7) нет   Да (8)

(9) Выбор следующего действия

(10) Построение гистограмм и подсчет самокоррекции

(11) Выбор следующего числа, участвующего в операции

(12) Анализ окончания процесса счета

(13) Выполнение следующего действия

(14) Печать результата

(15) Пересылка результата на место исходного числа

(16) Останов

Key: (1). Selection of the initial number A. (2). Selection of number of basis/base with distorted digit. (3). Obtaining distorted number A. (4). Determination of alternative set A. (5). Determination of

intersection of alternative sets. (6). Analysis of end of retraction.
(7). No. (8). Yes. (9). Selection of following operation. (10).
Construction of histograms and calculation of self correction. (11).
Selection of following number, which participates in operation. (12).
Analysis of end of process of calculation. (13). Execution of
following operation. (14). Printing result. (15). Sending of result
for place of initial number. (16). Stop.

Page 213.

2. Bases/bases go out of order randomly according to preset law
of distribution.

For each model of short duration failures was counted the length
of chain of operations, necessary for the localization of the place
of short duration failure. Results were obtained in the form of the
histograms of the frequencies of the convergence for the fixed values
of lengths of chain. On the basis of these histograms were
constructed the graph/diagrams of the dependences of probabilities it
was discovered and the correction of the error on operation number in
the circuit, and also on the length of chain with the short duration
failures in different bases/bases. Besides this was conducted the
calculation of medium chain lengths and was constructed the
graph/diagram of the dependence of medium chain length on the value

of basis/base, digit on which was erroneous.

Findings made it possible to also construct the dependences of the probabilities of localization of the place of the error as function of the length of chain of operations for different values of bases/bases.

The analysis of the results of the simulation conducted shows that the retraction of alternative sets always descends and gives the single-valued determination of the unknown basis/base. However, the build-up/growth of the probability of convergence strongly depends on the value of basis/base, on which occurred the error. Similar pattern occurs also for the probability of self correction, treated as a special case of the convergence of alternative sets.

If for small bases/bases (2 3, 5, 7) bulk of alternative sets during the calculation of circuit descends on the second or thrird operation, moreover maximum falls to the first operation, i.e., immediately for the self correction, then for more senior bases/bases (29, 31, 37, 41) occurs the shift/shear of maximum value for third operation and sharp decrease of possible self corrections. This, in particular, it is explained by the decrease of the probability of obtaining zero with the distorted basis/base and the more even distribution of these zeros all over the aggregate of the

results of the operations of circuit. Analogously the probability of
localization of the place of error with an increase in the length of
chain more rapidly approaches 1 for small bases/bases. If for
basis/base $p = 2$ the probability of localization of error for two
operations is equal to 0.73, then for $p = 41$ it is reduced to 0.28
i.e. almost three times. Yes even very character of dependence shows
that until the values of bases/bases are changed comparatively
smoothly (2, 3, 5, 7) that and curved sufficiently steady, and with a
sharp increase in the value of basis/base from 13 to 29 and further
to 41 curves it sharply falls downward.

Page 214.

With an increase in the length of chain the probability of
localization of the place of error increasingly less depends on the
value of basis/base and approximately/exemplarily at the length of
chain in 11-12 operations probabilities are equalized to the value,
equal to one.

That presented makes it possible to draw the conclusion that the
method of the contraction of the alternative aggregates of the
results of calculating the consecutive operations of circuit makes it
possible to localize the place of the error at the maximum length of
chain into 12 operations. However, average length of chain composes

4-5 operations.

The retraction of alternative sets can be somewhat accelerated, on the basis of the following considerations. In view of the fact that medium chain length increases with the value of bases/bases, it is expedient to increase the reliability of operation in the large bases/bases by one or the other technical means, at least even due to the decrease of the reliability of small bases/bases. In this case the short duration failures will occur predominantly on small bases/bases and, consequently will be accelerated the contraction of alternative to the place of error. In accordance with what has been said were simulated the retractions with the equiprobable short duration failures and independent of the value of bases/bases with the more probable short duration failures for small bases/bases. The results of simulation show the noticeable acceleration of contraction in the second case. Medium chain length is here equal to three operations.

Further was simulated the method of localization of the place of error on the hypothesis accepted, namely on any of the bases/bases, entering the alternative set of an incorrect number, is done correction and on the obtained correct number are implemented further operations of circuit. It is assumed that the incorrectly corrected number must not lead to the true results in the operations of

circuit.

Simulation was produced on the block diagram, represented on page 215.

It was conducted under the same conditions as the simulation of the retraction of alternative sets.

The analysis of obtained results shows that also by the method of hypotheses is reached satisfactory localization of the place of error, moreover in contrast to the method of the contraction of alternative sets the probability of localization of the place of error barely depends on the value of basis/base, according to which occurred the short duration failure.

Page 215.

A change in the value of this probability with an increase in the basis/base is so insignificant that virtually is not had an effect on the average/mean value of the length of chain, necessary for the localization of error, which in the method of hypotheses composes two operations for the short duration failure on any of the bases/bases. As far as length of chain is concerned maximum, then it in the method of hypotheses is equal to six operations.
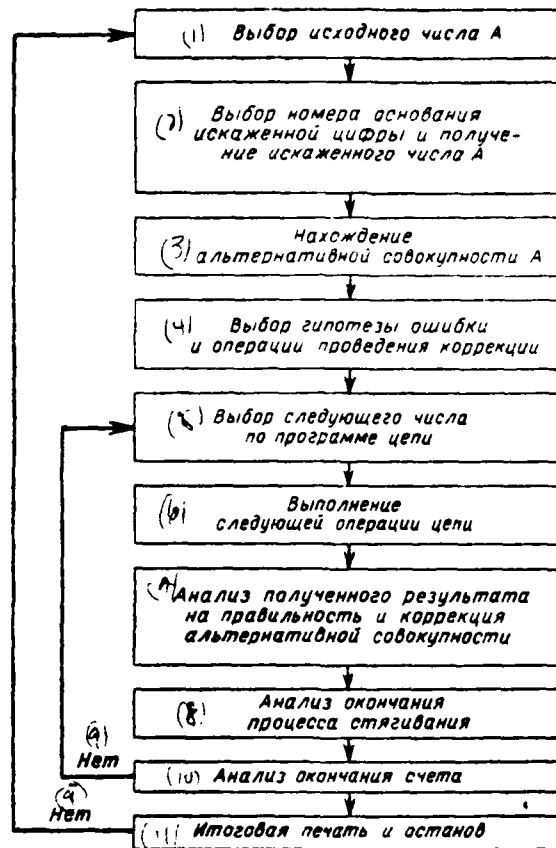
Key: (1). Selection of the initial number A. (2). Selection of number of basis/base of distorted digit and obtaining distorted number A. (3). Determination of alternative set A. (4). Selection of hypothesis of error and operation of conducting correction. (5). Selection of following number according to program of circuit. (6). Execution of following operation of circuit. (7). Analysis of obtained result for correctness and correction of alternative set. (8). Analysis of end

of retraction. (9). No. (10). Analysis of termination of calculation.
(11). Concluding printing and stop.

Page 216.

Thus, it is possible to draw the conclusion that the method of
hypotheses accelerates the process of localization of the error both
on the average and on the maximum, approximately/exemplarily doubly
in comparison with the method of the contraction of alternative sets.
Thus, with the fulfillment of three operations the probability of
localization of the error in the method of contraction composes 0.62,
and in the method of hypotheses this probability is equal to 0.965.

However, with the noted advantages the method of hypotheses is
more complicated on its realization both in the equipment sense and
algorithmically in comparison with the method of the contraction of
alternative sets. While the latter does not interrupt/break the
natural course of the process of calculations according to the
program, but seemingly in parallel are monitored it, the method of
hypotheses can in a number of cases require the discontinuity of
process and its return at the beginning of the reception of
hypothesis. Therefore it is considered by advisable to use the
combined process.

In particular, it is possible the large foundations for checking by the method of hypotheses and to exclude them from the alternative set, and for the remaining part of the alternative set to use the method of contraction.

The combined method also was simulated and were the findings, which characterize the parameters of the process of localization of the place of the error in the dependence on the relationship/ratio of the parts of the alternative set, processed by different methods. The analysis of these data clearly shows that the use/application of the combined method is very efficient. A quantity of excluded bases/bases is different during different capacities of alternative sets and different distribution them small and large bases/bases. Optimum is located near 0.4 from a quantity of bases/bases, entering the alternative set. In this case the medium chain length, necessary for the localization of error, will compose two operations, and the probability of localization of the error with six operations in the circuit is equal to 0.975.

Page 217.

Chapter 5.

ALGORITHMS OF THE EXECUTION NONMODULAR OPERATIONS.

Does not cause doubt the efficiency of the use/application of a
system of residual classes in the implementation of the majority of
arithmetic operations.

Somewhat more complicatedly proceeds matter with the execution
of nonmodular (positional) operations, which require the knowledge of
the value of entire number as a whole.

Thus, during the determination of the sign of a number, with the
fulfillment of the arithmetic comparison of two numbers, in certain
cases of division, with the rounding we should have information about
the value of entire number or, which is the same thing, it is
necessary to know the location of a number in the numerical range.

In this case, as a rule, to us it suffices to know the number of interval j, in which is located a number.

For the introduction of the sign of a number entire numerical range we divide/mark off into two parts and on that, in which of the parts it lies/rests the number in question, we judge its sign. Here knowing the number of interval $\left[j\frac{P}{p_n}, (j-1)\frac{P}{p_n} \right)$ in which is arranged/located a number, we know its sign.

Being congruent/equating with respect to the value two numbers, we judge that, which of the numbers more on the sign of difference.

The knowledge of the numbers of the intervals in which are arranged/located the operands, makes it possible to simplify the process of comparison, namely: if numbers lie/rest at the different intervals, then of them large is the number, which lies at the interval with the large number and, etc.

Page 218.

Until now, they used in the examination of nonmodular operations by some values, which characterize entire number as a whole: rank, and it is later by trace, by character.

In present chapter it is proposed to consider some algorithms of the determination of minimum trace or character of a number, and also the number interval, in which is arranged/located a number, for the purpose of the efficient realization of nonmodular operations.

§5.1. Method of weight characteristics.

Let us introduce the concept of the weight of a minimum pseudo-orthogonal number.

Definition. By the weight of the minimum pseudo-orthogonal number

$$M_{\alpha_i} = (0, 0, \ldots, 0, \alpha_i, 0, \ldots, S_{\alpha_i}^*)$$

we will understand correct binary fraction with a length of 1:

$$m_{\alpha_i}^l = \varepsilon_{\alpha_i}^{(1)} 2^{-1} + \varepsilon_{\alpha_i}^{(2)} 2^{-2} + \ldots + \varepsilon_{\alpha_i}^{(l)} 2^{-l},$$

where

$$\varepsilon_{\alpha_i}^{(j)} = \begin{cases} 0, \text{ если } (2^{j-1}\alpha_i, \ 2^{j-1}\alpha_i) - \text{правильная пара}, \\ 1, \text{ в противном случае} \end{cases}$$

Key: (1). if. (2). correct pair. (3). otherwise.

with j=1, 2, ..., l.

The connection of the value of a minimum pseudo-orthogonal number with its weight is determined by the following theorem.

Theorem 5.1. If in the standardized/normalized system of the bases/bases

$$p_1, \ p_2, \ \ldots, \ p_n$$

is preset the minimum pseudo-orthogonal number

$$M_{\alpha_i} = (0, \ 0, \ \ldots, \ \alpha_i, \ \ldots, \ S^*_{\alpha_i})$$

with a weight of m_{α_i} with a length of l

$$m^l_{\alpha_i} = \varepsilon^{(1)}_{\alpha_i} 2^{-1} + \varepsilon^{(2)}_{\alpha_i} 2^{-2} + \ldots + \varepsilon^l_{\alpha_i} 2^{-l},$$

then value M_{α_i} is connected with its weight with the following relationship/ratio:

$$m^l_{\alpha_i} \frac{\mathscr{P}}{p_n} < M_{\alpha_i} < m^l_{\alpha_i} \frac{\mathscr{P}}{p_n} + 2^{-l} \frac{\mathscr{P}}{p_n} . \qquad (5.1)$$

Page 219.

Proof. According to the determination of the weight of a number, if $\varepsilon^{(1)}_{\alpha_i} = 1$, pair (α_i, α_i) is incorrect, i.e., during the addition of initial minimum pseudo-orthogonal number M_{α_i} of very with itself we will obtain

$$2M_{\alpha_i} \geqslant \frac{\mathscr{P}}{p_n}$$

either

$$M_{\alpha_i} \geqslant 2^{-1} \frac{\mathscr{P}}{p_n} .$$

and if $\varepsilon^{(1)}_{\alpha_i} = 0$, than pair (α_i, α_i) is correct, whence

$$0 \leqslant 2M_{\alpha_i} < \frac{\mathscr{P}}{p_n}$$

or

$$M_{\alpha_i} < 2^{-1} \frac{\mathscr{P}}{p_n} .$$

Joining these inequalities, we can write

$$\varepsilon_{\alpha_i}^{(1)} 2^{-1} \frac{\mathscr{P}}{p_n} \leqslant M_{\alpha_i} < \varepsilon_{\alpha_i}^{(1)} 2^{-1} \frac{\mathscr{P}}{p_n} + 2^{-1} \frac{\mathscr{P}}{p_n} .$$

It is logical that a similar inequality can be written for any $j \leqslant 1$

$$\varepsilon_{\alpha_i}^{(j)} 2^{-1} \frac{\mathscr{P}}{p_n} \leqslant M_{2^{j-1}\alpha_i} < \varepsilon_{\alpha_i}^{(j)} 2^{-1} \frac{\mathscr{P}}{p_n} + 2^{-1} \frac{\mathscr{P}}{p_n} . \qquad (5.2)$$

Let us use further the method of induction. Let us assume that (5.1) it is correct for $l=j-1$. Let us show that it is correct then for $l=j$. Let take place

$$m_{\alpha_i}^{j-1} \cdot \frac{\mathscr{P}}{p_n} \leqslant M_{\alpha_i} < m_{\alpha_i}^{j-1} \frac{\mathscr{P}}{p_n} + 2^{-(j-1)} \frac{\mathscr{P}}{p_n} . \qquad (5.3)$$

Let us first of all note that

$$M_{2^{j-1}\alpha_i} = 2^{j-1} M_{\alpha_i} - \left[2^{j-1} \frac{M_{\alpha_i}}{\mathscr{P}/p_n} \right] \frac{\mathscr{P}}{p_n} .$$

But on the basis (5.3) we can write

$$\left[2^{j-1} \frac{M_{\alpha_i}}{\mathscr{P}/p_n} \right] \frac{\mathscr{P}}{p_n} = 2^{j-1} m_{\alpha_i}^{j-1} \frac{\mathscr{P}}{p_n} ,$$

whence

$$M_{2^{j-1}\alpha_i} = 2^{j-1} M_{\alpha_i} - 2^{j-1} M_{\alpha_i}^{j-1} \frac{\mathscr{P}}{p_n} . \qquad (5.4)$$

Page 220.

Then inequality (5.2) can be rewritten in the form

$$\varepsilon_{\alpha_i}^{(j)} 2^{-1} \frac{\mathscr{P}}{p_n} + 2^{j-1} m_{\alpha_i}^{j-1} \frac{\mathscr{P}}{p_n} \leqslant 2^{j-1} M_{\alpha_i} < \varepsilon_{\alpha_i}^{(j)} 2^{-1} \frac{\mathscr{P}}{p_n} +$$
$$+ 2^{-1} \frac{\mathscr{P}}{p_n} + 2^{j-1} m_{\alpha_i}^{j-1} \frac{\mathscr{P}}{p_n}$$

or

$$m_{\alpha_i}^{j-1} \frac{\mathscr{P}}{p_n} + \varepsilon_{\alpha_i}^{(j)} 2^{-j} \frac{\mathscr{P}}{p_n} \leqslant M_{\alpha_i} < m_{\alpha_i}^{j-1} \frac{\mathscr{P}}{p_n} + \varepsilon_{\alpha_i}^{(j)} 2^{-j} \frac{\mathscr{P}}{p_n} + 2^{-j} \frac{\mathscr{F}}{p_n} .$$

However, since

$$m_{\alpha_i}^{j} = m_{\alpha_i}^{j-1} + \varepsilon_{\alpha_i}^{(j)} 2^{-j},$$

that

$$m_{\alpha_i}^{j} \frac{\mathscr{P}}{p_n} \leqslant M_{\alpha_i} < m_{\alpha_i}^{j} \frac{\mathscr{P}}{p_n} + 2^{-j} \frac{\mathscr{F}}{p_n} .$$

that also proves assertion (5.1) of theorem.

Corollary 1. If for this basis/base p_i it will be found integer π_i, satisfying the comparison

$$2^{\pi_i} \equiv 1 \ (\mathrm{mod}\ p_i),$$

then occurs the following equality

$$(2^{\pi_i} - 1) M_{\alpha_i} = k \frac{\mathscr{P}}{p_n} , \qquad (5.5)$$

where k - integer.

Subsequently value π_i we will call the length of weight m_{α_i}. Actually/really, assuming/setting in (5.4) $j - 1 = \pi_i$, we will obtain

$$M_{2^{\pi_i}\alpha_i} = 2^{\pi_i} M_{\alpha_i} - 2^{\pi_i} m_{\alpha_i}^{\pi_i} \frac{\mathscr{P}}{p_n} \qquad (5.6)$$

or, taking into account that, regarding π_i, has the place

$$M_{2^{\pi_i}\alpha_i} = M_{\alpha_i}.$$

we can register (5.6) in the form

$$(2^{\pi_i} - 1) M_{\alpha_i} = 2^{\pi_i} m_{\alpha_i}^{\pi_i} \frac{\mathscr{P}}{p_n} , \qquad (5.7)$$

which coincides with (5.5) with

$$k = 2^{\pi_i} m_{\alpha_i}^{\pi_i}.$$

Page 221.

Corollary 2. From (5.7) ensues/escapes/flows out in this case representation M_{α_i} in the form

$$M_{\alpha_i} = \frac{2^{\pi_i} m_{\alpha_i}^{\pi_i}}{2^{\pi_i} - 1} \frac{\mathcal{P}}{p_n} . \qquad (5.8)$$

Let to us be is preset number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

We form sum M_A of the minimum pseudo-orthogonal numbers

$$M_{\alpha_1} = (\alpha_1, 0, \ldots, 0, S_{\alpha_1}^*).$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$M_{\alpha_{n-1}} = (0, 0, \ldots, \alpha_{n-1}, S_{\alpha_{n-1}}^*).$$

each of which has a weight $m_{\alpha_i}^{\pi_i}$ (i=1, 2, ..., n-1), i.e.,

$$M_A = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A) = \sum_{i=1}^{n-1} M_{\alpha_i}. \qquad (5.9)$$

Let us assume that the least common multiple π of values $\pi_1, \pi_2, \ldots, \pi_{n-1}$ is such, that is satisfied the condition

$$2^{\pi} \equiv 1 \;(\mathrm{mod}\; p_i),$$
$$i = 1, 2, \ldots, n-1, \qquad (5.10)$$

then, passing for each of the selected minimum pseudo-orthogonal numbers to the weight by length π, we obtain in accordance with (5.5)

$$M_{\alpha_i} = \frac{2^{\pi} m_{\alpha_i}^{\pi}}{2^{\pi} - 1} \frac{\mathcal{P}}{p_n} .$$

after which the expression of signs the form

$$M_A = \frac{2^\pi}{2^\pi - 1} \frac{\mathscr{F}}{p_n} \sum_{i=1}^{n-1} m_{\alpha_i}^\pi. \qquad (5.11)$$

Determination. By weight m_A^π of number A of length π we will call the sum of weights the length π of the minimum pseudo-orthogonal numbers where value π satisfies (5.10), the components this number A, i.e.,

$$m_A^\pi = \sum_{i=1}^{n-1} m_{\alpha_i}^\pi.$$

Page 222.

Then expression (5.11) can be registered in the form

$$M_A = \frac{2^\pi m_A^\pi}{2^\pi - 1} \frac{\mathscr{P}}{p_n}, \qquad (5.12)$$

Let us formulate the following theorem.

Theorem 5.2. (about the minimum trace of a number). If in the standardized/normalized system of bases/bases is preset the number

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$$

with a weight of m_A^π by length π, not multiple to value $2^\pi - 1$, and by trace S_A, then the minimum trace of the preset number is determined by the equality

$$S_A^* = \left(S_A - \left[\frac{2^\pi m_A^\pi}{2^\pi - 1} \right] \right) (\bmod p_n). \qquad (5.13)$$

Proof. In accordance with (5.12) and theorem conditions we have

$$\left[\frac{2^\pi m_A^\pi}{2^\pi-1}\right]\frac{\mathscr{P}}{p_n}<M_A<\left(\left[\frac{2^\pi m_A^\pi}{2^\pi-1}\right]+1\right)\frac{\mathscr{P}}{p_n}.$$

Consequently, number M_A is located in the interval, distant behind interval $\left[0,\frac{\mathscr{P}}{p_n}\right)$ to value $\left[\frac{2^\pi m_A^\pi}{2^\pi-1}\right]$ of intervals.

Since the minimum form A* of number A has a trace S_A^*, and number A has a trace S_A, then

$$M_A=A^*+(S_A-S_A^*)\,(\mathrm{mod}\,p_n)\,\frac{\mathscr{P}}{p_n},$$

but hence

$$S_A-S_A^*=\left[\frac{2^\pi m_A^\pi}{2^\pi-1}\right](\mathrm{mod}\,p_n),$$

that also composes the assertion of theorem.

The method examined makes it possible to accurately determine value of the minimum trace of a number, and therefore, the number of the interval in which it is arranged/located. By the comparison of values a_n, S_A^* and S_A we also accurately determine the value of the character of a number.

Page 223.

However, for the operation with numbers in the sufficiently large range the length of weight π in general is obtained sufficiently large and the formation/education of weight m_A^π

requires the addition of long numbers (weights), which impedes the practical application of this method.

Therefore the proposed method can be examined into somewhat other plan/layout, namely let us assign the weights of small length and will try to narrow down the region of the uncertainty/indeterminancy of the minimum trace of a number.

Let us select length of the weight of a number, equal 1. Then the weight of a minimum pseudo-orthogonal number is defined as m'_i, i.e. it decreases by value

$$m_{\alpha_i}^\pi - m_{\alpha_i}^l = \varepsilon_{\alpha_i}^{(l+1)}2^{-(l+1)} + \ldots + \varepsilon_{\alpha_i}^{(\pi)}2^{-\pi} < 2^{-l}.$$

and the weight of number A will be defined as

$$m_A^l = m_A^\pi - \sum_{i=1}^{n-1} (m_{\alpha_i}^\pi - m_{\alpha_i}^l)$$

or

$$m_A^l < m_A^\pi < m_A^l + (n-1)2^{-l}.$$

whence

$$\left[\frac{2^\pi m_A^l}{2^\pi - 1}\right] < S_A - S_A^* \pmod{p_n} < \left[\frac{2^\pi}{2^\pi - 1}(m_A^l + (n-1)2^{-l})\right].$$
(5.14)

Since it is assumed that $\pi \gg 1$, then with a sufficient degree of accuracy it is possible to count

$$\frac{2^\pi}{2^\pi - 1} \approx 1.$$

Value 1 let us select in such a way that would be satisfied the

inequality

$$(n-1)\,2^{-l} \leqslant 1$$

or

$$l \geqslant \log_2(n-1).$$

Then (5.14) signs the form

$$[m_A^l] \leqslant S_A - S_A^* \,(\mathrm{mod}\ p_n) \leqslant [m_A^l + 1],$$

i.e. the minimum trace of a number can have values either

$$S_A^* = (S_A - [m_A^l])\,(\mathrm{mod}\ p_n),$$

or

$$S_A^* = (S_A - [m_A^l] - 1)\,(\mathrm{mod}\ p_n).$$

As we see, the region of the possible values of the minimum trace of a number substantially decreased.

Page 224.

§5.2. Method of nulling.

In chapter 4 has already been discussed the method of nulling, during numbering of the interval in which is arranged/located the interesting us number. Was there formulated the theorem about the independence the result of nulling from the procedure of process. In the present section is assumed the more thorough examination of this method.

Determination. Nulling we will call such method of the transformation of the number, preset in the system of residual classes, with which in each stage of transformation a number of zero digits in the representation of a number increases also in this case is ensured the nonappearance of the converted number beyond the borders of that interval of the numerical range in which it is arranged/located.

Determination. A minimum number of nulling M_{ij} we will call small from numbers of the form

$$M_{ij} = (0, 0, \ldots, 0, \alpha_i^{(j)}, \alpha_{i+1}^{(j)}, \ldots, \alpha_n^{(j)}), \qquad (5.15)$$

moreover

$$i = 1, 2, \ldots, n-1,$$
$$j = 1, 2, \ldots, p_i - 1.$$

It is obvious that in all minimum numbers of nulling for the preset system of bases/bases it will be

$$p_1 + p_2 + \ldots + p_{n-1} - (n-1)$$

numbers.

Theorem 5.3. (The limit theorem of nulling). Let at the standardized/normalized system of bases/bases $p_1, p_2, \ldots, p_n$ he is preset the number

$$A = (0, \ldots, 0, \alpha_i, \alpha_{i+1}, \ldots, \alpha_n),$$

lying at the interval

$$\left[t \frac{\mathcal{P}}{p_n}, \ (t+1) \frac{\mathcal{P}}{p_n} \right)$$

and let be is preset a minimum number of nulling

$$M_{i(p_i - \alpha_i)} = (0, \ldots, 0, p_i - \alpha_i, \alpha_{i-1}^{(p_i - \alpha_i)}, \ldots, \alpha_n^{(p_i - \alpha_i)}).$$

Then the sum of these numbers

$$A + M_{i(\nu_i - \alpha_i)}$$

either lies/rests at the same interval or on its right border.

Page 225.

Proof. Actually/really, addition to number A of a minimum number of nulling $M_{i(p_i - \alpha_i)}$ cannot form the number, greater

$$(t + 1) \frac{\mathscr{P}}{p_n}.$$

If would occur the inequality

$$A + M_{i(p_i - \alpha_i)} > (t + 1) \frac{\mathscr{P}}{p_n},$$

it would be possible from numbers of form (5.15) to select number $T_{i(p_i - \alpha_i)}$, satisfying the condition

$$T_{i(p_i - \alpha_i)} = (t + 1) \frac{\mathscr{P}}{p_n} - A.$$

But then would take place the inequality

$$T_{i(p_i - \alpha_i)} < M_{i(p_i - \alpha_i)},$$

which contradicts the determination of a minimum number of nulling. Thereby it is proven, which

$$A + M_{i(p_i - \alpha_i)} \leqslant (t + 1) \frac{\mathscr{P}}{p_n},$$

that also composes the assertion of theorem.

Theorem 5.4. If in the standardized/normalized system of

bases/bases is preset the number

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$$

and if by nulling number A minimum numbers of nulling $M_{i(p_i - \alpha_i)}$
obtained a number of form

$$(0, 0, \ldots, 0, \alpha_n^{(n-1)}),$$

then the minimum trace of number A is determined by the equality

$$S_A^* = (\alpha_n - \alpha_n^{(n-1)} + 1)\,(\mathrm{mod}\,p_n). \qquad (5.16)$$

Proof. Consecutively/serially applying the theorem of nulling
5.3 to number A and to obtained intermediate results (n-1) of times,
we will obtain:

$$A_1 = A + M_{1(p_1 - \alpha_1)} = (0, \alpha_2^{(1)}, \alpha_3^{(1)}, \ldots, \alpha_{n-1}^{(1)}, \alpha_n^{(1)}).$$
$$A_2 = A_1 + M_{2(p_2 - \alpha_2^{(1)})} = (0, 0, \alpha_3^{(2)}, \ldots, \alpha_{n-1}^{(2)}, \alpha_n^{(2)}).$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$A_{n-1} = A_{n-2} + M_{n-1,\,(p_{n-1} - \alpha_{n-1}^{(n-2)})} = (0, 0, \ldots, 0, \alpha_n^{(n-1)}).$$

Page 226.

In this case it is assumed that in the case when nulled digit is
equal to zero, the corresponding minimum number of nulling is equal
to zero.

Thus we obtain, that number A is located in the interval

$$\left[(\alpha_n^{(n-1)} - 1)\,\frac{\mathscr{P}}{p_n},\; \alpha_n^{(n-1)}\,\frac{\mathscr{P}}{p_n} \right).$$

Since minimum trace S_A^* of number A is this value of digit on

the latter/last basis/base with which a number is located in the
first interval, then minimum trace can be determined according to
value α_n and $\alpha_n^{(n-1)}$. let us consider the possible relationships/ratios
between α_n and that obtained $\alpha_n^{(n-1)}$.

Case 1.   Let $\alpha_n \geqslant \alpha_n^{(n-1)} - 1$.

Then regarding the minimum trace it follows

$$S_A^* = \alpha_n - (\alpha_n^{(n-1)} - 1),$$

which coincides with (5.16).

Case 2. $\alpha_n < \alpha_n^{(n-1)} - 1$.

Then the minimum trace of number A is determined so

$$S_A^* = \alpha_n + p_n - (\alpha_n^{(n-1)} - 1),$$

that also it coincides with (5.16).

Until now, was examined the process of consecutive nulling.

For the purpose of the economy of the time of the execution of
this procedure in each stage the nulling can be carried out
simultaneously through two digits. True, for this will be required
certain increase in the quantity of minimum numbers of nulling.

Best combination pair, into which should be joined the bases/bases for each stage of nulling, is determined by the following theorem.

Theorem 5.5. If it is preset 2s integers a_i (i=1, 2, ..., 2s), which satisfy the inequalities

$$a_1 < a_2 < \ldots < a_{2s-1} < a_{2s}, \qquad (5.17)$$

and if the sum of the pair products, formed from these numbers

$$S = \sum_{(i \neq j) = 1}^{2s} a_i a_j,$$

is such, that each of the numbers a_i is encountered in one and only one member of this sum, then from all possible such sums, formed by different groupings of members a_i, of the smallest is the sum

$$S = a_1 a_{2s} + a_2 a_{2s-1} + \ldots + a_s a_{s+1}. \qquad (5.18)$$

Page 227.

Proof. Let us demonstrate first the validity of this assertion for four numbers

$$a_1 < a_2 < a_3 < a_4.$$

We form from these numbers all possible sums of the pair products:

$$S_1 = a_1 a_2 + a_3 a_4.$$
$$S_2 = a_1 a_3 + a_2 a_4,$$
$$S = a_1 a_4 + a_2 a_3.$$

Let us compute the differences
$$S_1 - S = (a_1 - a_3)(a_2 - a_4) > 0,$$
$$S_2 - S = (a_1 - a_2)(a_3 - a_4) > 0.$$

Hence it follows that S is the smallest sum. Let us consider now sum of $\overline{S}$, formed by the arbitrary grouping of terms a_i (i = 1, 2, ..., 2s):

$$\overline{S} = a_{j_1} a_{j_2} + a_{j_3} a_{j_4} + \ldots + a_{j_{2s-1}} a_{j_{2s}}.$$

Here $a_{j_1}, a_{j_2}, \ldots, a_{j_{2s}}$ - number of (5.17).

If in this sum is not encountered products $a_1 a_{2s}$. then it is possible in it to select the sum of the following two members:

$$a_1 a_{j_r} + a_{2s} a_{j_\tau}.$$

After replacing this sum of $\overline{S}$ on $a_1 a_{2s} + a_{j_r} a_{j_\tau}$, we will obtain the new sum of $\overline{S}_1$ for which occurs the inequality

$$\overline{S}_1 < \overline{S}.$$

Further, in $\overline{S}_1$ we find two members $a_2 a_{j_k} + a_{2s-1} a_{j_m}$ and, after replacing them by $a_2 a_{2s-1} + a_{j_k} a_{j_m}$. we will obtain sum of $\overline{S}_2$, where $\overline{S}_2 < \overline{S}_1$. Continuing in this way to minimize the obtained sums, let us arrive at (5.18).

Corollary.

Page 228.

If it is preset 2s+1 the integers, which satisfy the condition

$$a_1 < a_2 < \ldots < a_{2s} < a_{2s+1},$$

where $a_1 > 1$, then the minimum sum of pairwise products in which each number a_i ($i=1, 2, \ldots, 2s+1$) enters into one and only one member of sum, has the form

$$S = a_1 a_{2s} + a_2 a_{2s-1} + \ldots + a_s a_{s+1} + a_{2s+1}. \quad (5.19)$$

Actually/really, supplementing term $a_0 = 1$, we change the sum in all in question per unit. Applying to the obtained numbers previous theorem, we obtain (5.19).

Note. Assertion, which sum (5.19) minimum, is correct for $a_1 = 1$, but in this case can exist even some combinations of the members of sums, which ensure the same minimum value of sum.

For example, for three numbers

$$a_1 < a_2 < a_3$$

can be formed the following sums:

$$S_1 = a_2 a_3 + a_1,$$
$$S_2 = a_1 a_3 + a_2, \quad (5.20)$$
$$S = a_1 a_2 + a_3,$$

difference in which will be

$$S_1 - S = (a_3 - a_1)(a_2 - 1) > 0,$$
$$S_2 - S = (a_3 - a_2)(a_1 - 1),$$

i.e. with $a_1 = 1$ we obtain $S_2 = S$, in other words both combinations of terms give the identical minimum value of sum.

In our case of the association of the basis of system for the economical carrying out of pair nulling we always have the low-order basis/base, greater than unity.

Let us give the examples, which illustrate the execution of consecutive and pair nulling.

Let us select for this purpose the system of the bases/bases

$$p_1 = 3; \quad p_2 = 5; \quad p_3 = 7; \quad p_4 = 13; \quad p_5 = 31.$$

For the consecutive nulling let us write out minimum numbers of nulling.

On basis/base $p_1 = 3$

$$M_{11} = (1, 1, 1, 1, 1) = 1,$$
$$M_{21} = (2, 2, 2, 2, 2) = 2.$$

On basis/base $p_2 = 5$:

$$M_{12} = (0, 1, 6, 6, 6) = 6 \quad M_{32} = (0, 3, 3, 3, 3) = 3$$
$$M_{22} = (0, 2, 5, 12, 12) = 12 \quad M_{42} = (0, 4, 2, 9, 9) = 9$$

Page 229.

On basis/base $p_3 = 7$:

$$M_{13} = (0, 0, 1, 2, 15) = 15 \quad M_{43} = (0, 0, 4, 8, 29) = 60$$
$$M_{23} = (0, 0, 2, 4, 30) = 30 \quad M_{53} = (0, 0, 5, 10, 13) = 75$$
$$M_{33} = (0, 0, 3, 6, 14) = 45 \quad M_{63} = (0, 0, 6, 12, 28) = 90$$

On basis/base $p_4 = 13$:

$M_{14} = (0, 0, 0, 1, 12) = 105$ $M_{74} = (0, 0, 0, 7, 22) = 735$

$M_{24} = (0, 0, 0, 2, 24) = 210$ $M_{84} = (0, 0, 0, 8, 3) = 840$

$M_{34} = (0, 0, 0, 3, 5) = 315$ $M_{94} = (0, 0, 0, 9, 15) = 945$

$M_{44} = (0, 0, 0, 4, 17) = 420$ $M_{104} = (0, 0, 0, 10, 27) = 1050$

$M_{54} = (0, 0, 0, 5, 29) = 525$ $M_{114} = (0, 0, 0, 11, 8) = 1155$

$M_{64} = (0, 0, 0, 6, 10) = 630$ $M_{124} = (0, 0, 0, 12, 20) = 1260$

For conducting the pair nulling, as it follows from the third theorem of nulling, to most economically join bases/bases into the following pairs: $p_1 p_4$ and $p_2 p_3$.

In this case the total quantity of necessary minimum numbers will be

$$S = p_1 p_4 + p_2 p_3 = 74.$$

Are conveniently placed them into the following tables.

The table

α_4	$\alpha_1 = 0$	$\alpha_1 = 1$	$\alpha_1 = 2$
0	(0, 0, 0, 0, 0)	(1, 3, 6, 0, 13)	(2, 1, 5, 0, 26)
1	(0, 2, 6, 1, 27)	(1, 1, 1, 1, 1)	(2, 4, 0, 1, 14)
2	(0, 0, 1, 2, 15)	(1, 3, 0, 2, 29)	(2, 2, 2, 2, 2)
3	(0, 3, 3, 3, 3)	(1, 1, 2, 3, 16)	(2, 4, 1, 3, 29)
4	(0, 0, 2, 4, 30)	(1, 4, 4, 4, 4)	(2, 2, 3, 4, 17)
5	(0, 3, 4, 5, 18)	(1, 1, 3, 5, 0)	(2, 0, 5, 5, 5)
6	(0, 1, 6, 6, 6)	(1, 4, 5, 6, 19)	(2, 2, 4, 6, 1)
7	(0, 3, 5, 7, 2)	(1, 2, 0, 7, 7)	(2, 0, 6, 7, 20)
8	(0, 1, 0, 8, 21)	(1, 4, 6, 8, 3)	(2, 3, 1, 8, 8)
9	(0, 4, 2, 9, 9)	(1, 2, 1, 9, 22)	(2, 0, 0, 9, 4)
10	(0, 1, 1, 10, 5)	(1, 0, 3, 10, 10)	(2, 3, 2, 10, 23)
11	(0, 4, 3, 11, 24)	(1, 2, 2, 11, 6)	(2, 1, 4, 11, 11)
12	(0, 2, 5, 12, 12)	(1, 0, 4, 12, 25)	(2, 3, 3, 12, 7)

α_3	$\alpha_2 = 0$	$\alpha_2 = 1$	$\alpha_2 = 2$
0	(0, 0, 0, 0, 0)	(0, 1, 0, 0, 19)	(0, 2, 0, 0, 7)
1	(0, 0, 1, 0, 23)	(0, 1, 1, 0, 10)	(0, 2, 1, 0, 29)
2	(0, 0, 2, 0, 14)	(0, 1, 2, 0, 1)	(0, 2, 2, 0, 20)
3	(0, 0, 3, 0, 5)	(0, 1, 3, 0, 24)	(0, 2, 3, 0, 11)
4	(0, 0, 4, 0, 27)	(0, 1, 4, 0, 15)	(0, 2, 4, 0, 2)
5	(0, 0, 5, 0, 18)	(0, 1, 5, 0, 6)	(0, 2, 5, 0, 25)
6	(0, 0, 6, 0, 9)	(0, 1, 6, 0, 28)	(0, 2, 6, 0, 16)

α_3	$\alpha_2 = 3$	$\alpha_2 = 4$
0	(0, 3, 0, 0, 25)	(0, 4, 0, 0, 13)
1	(0, 3, 1, 0, 16)	(0, 4, 1, 0, 4)
2	(0, 3, 2, 0, 8)	(0, 4, 2, 0, 26)
3	(0, 3, 3, 0, 30)	(0, 4, 3, 0, 17)
4	(0, 3, 4, 0, 21)	(0, 4, 4, 0, 8)
5	(0, 3, 5, 0, 12)	(0, 4, 5, 0, 0)
6	(0, 3, 6, 0, 3)	(0, 4, 6, 0, 22)

Page 230.

Example. To lead the consecutive nulling of number $A = (0, 1, 3, 4, 13)$ and to determine its minimum trace.

We carry out the nulling:

$$A_1 = A - 0 = (0, 1, 3, 4, 13).$$
$$A_{12} = A_1 + M_{24} = (0, 1, 3, 4, 13) + (0, 4, 2, 9, 9) = (0, 0, 5, 0, 22),$$
$$A_{123} = A_{12} + M_{32} = (0, 0, 5, 0, 22) + (0, 0, 2, 4, 30) = (0, 0, 0, 4, 21),$$
$$A_{1234} = A_{123} + M_{49} = (0, 0, 0, 4, 21) + (0, 0, 0, 9, 15) = (0, 0, 0, 0, 5).$$

Since $\alpha_n = 13$, and $\alpha_n^{(n-1)} = 5$, from (5.16) we obtain, that

$$S_A^* = 9.$$

Example. To lead the pair nulling of number $A = (0, 1, 3, 4, 13)$ and to determine its minimum trace.

We carry out the nulling

$$A_{14} = (0, 1, 3, 4, 13) + (0, 4, 2, 9, 9) = (0, 0, 5, 0, 22),$$
$$A_{1234} = (0, 0, 5, 0, 22) + (0, 0, 2, 0, 14) = (0, 0, 0, 0, 5).$$

From (5.16) it follows that $S_A^* = 9$.

§5.3. Method of the evaluation of intervals.

Determination. We will call critical the case when occurs the relationship/ratio

$$|\alpha_n - S_A^*| \leqslant n - 2 - \omega, \qquad (5.21)$$

where ω - number of zero digits in the representation of number A.

Page 231.

The hence critical case for number A occurs with the following of the value of number A:

case 1

$$A = a,$$
$$A = \frac{\mathcal{P}}{p_n} + a,$$
$$A = 2\frac{\mathcal{P}}{p_n} + a.$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$A = (n - 2 - \omega)\frac{\mathcal{P}}{p_n} + a.$$

Case of 2

$$A = (p_n - 1)\frac{\mathcal{P}}{p_n} + a,$$
$$A = (p_n - 2)\frac{\mathcal{P}}{p_n} + a.$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$A = (p_n - n + 2 + \omega)\frac{\mathcal{P}}{p_n} + a.$$

Here a - whole non-negative number, which satisfies the condition

$$0 \leqslant a < \frac{\mathcal{P}}{p_n}.$$

Determination. The presence of the situation when number A relates to the first case, we will subsequently call first type criticality, the situation during which number A relates to the second case, we will call second type criticality.

Number itself A we will call first or second type critical number or simply critical number.

In other words the critical case occurs for the numbers, which lie in $(n-2-\omega)$ the intervals from both sides of interval $\left[0, \frac{\mathcal{P}}{p_n}\right)$, where is located the minimum form of a number.

With $\omega = n-2$ we obtain $k = n-2-\omega = 0$. In other words if a number have $n-2$ zero digits, then the critical case is degenerated into equality $a_n = S_A^*$. the determining minimum pseudo-orthogonal number.

Logical therefore to trace the methods, directed toward the decrease of value $k = n-2-\omega$, the characterizing zone uncertainty/indeterminancy.

In view of constancy n, which is determining a number of basis of system, decrease k can be reached only due to an increase ω, i.e., this transformation of number A, with which increases a number of its zero digits. On this rests the described above method of nulling.

Page 232.

1.0

1.1

1.25 1.4 1.6

4.5 2.8 2.5

3.2 2.2

3.6

4.0 2.0

1.8
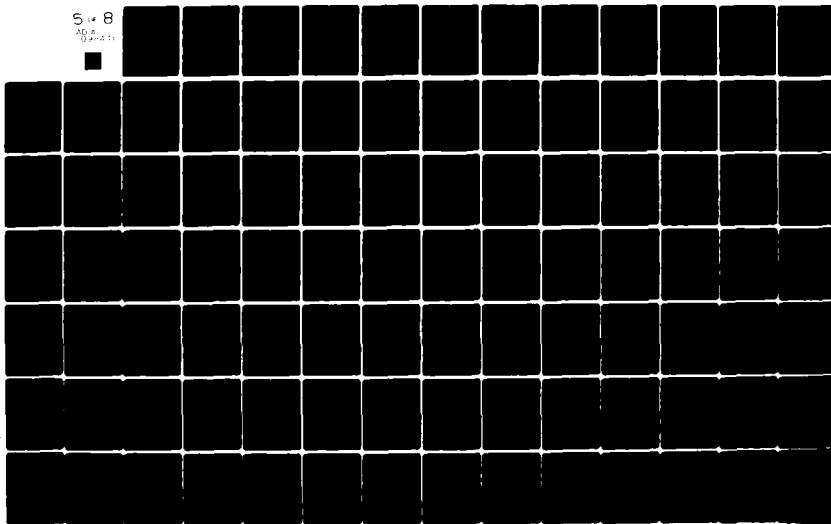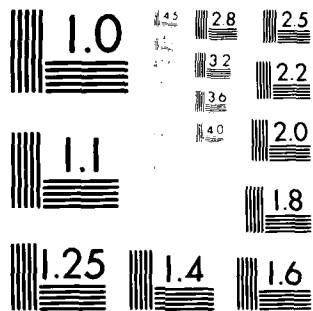
MICROCOPY RESOLUTION TEST CHART

Let us consider a somewhat different way of disclosing/expanding
the uncertainty/indeterminancy.

Theorem 5.7. If in the standardized/normalized system of
bases/bases $p_1, p_2, \ldots, p_n$ is preset critical number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and
if for basis/base p_i $(i=1, 2, \ldots, (n-1))$, is satisfied the
condition

$$p_i(n-1) + n - 3 \leqslant p_n, \qquad (5.22)$$

then for number $\widetilde{A}$, defined as

$$\widetilde{A} = A p_i,$$

either does not occur the critical case or occurs a criticality of
the same type, as for number A.

Proof. First type greatest critical number is the number

$$A_{max}^{I} = (n-1)\frac{\mathscr{P}}{p_n} - 1;$$

a hence smallest noncritical number it will be

$$A_{min}^{I} = (n-1)\frac{\mathscr{P}}{p_n}.$$

By second type smallest critical number it is

$$A_{min}^{II} = (p_n - n + 2)\frac{\mathscr{P}}{p_n} + 1,$$

whence the greatest noncritical number it will be

$$A_{max}^{II} = (p_n - n + 2)\frac{\mathscr{P}}{p_n}.$$

If as a result of the multiplication of the initial number A by
basis/base p_i product $\widetilde{A} = A p_i$ ceases to be susceptible, then it is
possible to establish/install the type of criticality only in such a

case, when the number domain of the first type of criticality,
multiplied by p_i, does not intersect with the region of second type
criticality, and the number domain of the second type of criticality,
multiplied by p_i, it does not intersect with the region of first type
criticality, in other words if occurs the following
relationship/ratio:

$$p_i(n-1)\frac{\mathscr{P}}{p_n} < (p_n - n + 3)\frac{\mathscr{P}}{p_n},$$

in which the border of second rejection region is determined by value
n-3, and not n-2 on the strength of the fact that the product of any
number to basis/base p_i has in its representation at least one zero
digit.

Page 233.

The given above relationship/ratio can be registered in the form
(5.22). It is logical that with satisfaction of condition (5.22)
number A, being multiplied by p_i, it cannot change the type of its
criticality to the opposite.

If after the multiplication of the critical number A by p_i the
product

$$\bar{A} = A p_i$$

is noncritical, then the type of the criticality of number A and its
character can be determined on the basis of the following theorem.

Theorem 5.8. (about the type of criticality) If in the
standardized/normalized system of the bases/bases where

$$p_n > p_i(n-1)$$

is preset number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ with trace S_A and if number Ap_i
with trace S_{Ap_i} and by character Δ_{Ap_i} it is not critical, then in the
case, if value

$$\theta = \Delta_{Ap_i} + \rho_1 - \rho_2 - \rho_3 \qquad (5.23)$$

is equal to zero or multiple p_i, number A is first type critical
number and its character is equal to

$$\Delta_A = \frac{\theta}{p_i}. \qquad (5.24)$$

Otherwise number A is second type critical number. Values ρ_1,
ρ_2, ρ_3 are determined by the expressions

$$\rho_1 = \sum_{i=1}^{p_i-1} \xi_{ii}, \quad \rho_2 = \sum_{i=1}^{p_i-1} \eta_{ii}, \quad \rho_3 = \sum_{i=1}^{p_i-1} \gamma_{ii}. \qquad (5.25)$$

Proof. Since number Ap_i is multiple p_i, then it can be divided
on p_i by simply step-by-step division. In this case will be obtained
the quotient C of the form

$$C = \frac{Ap_i}{p_i} = (\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, X, \alpha_{i+1}, \ldots, \alpha_n).$$

which coincides with number A in all to significant digits, except
digit in basis/base p_i. Relative to digit on basis/base p_i occurs
the uncertainty/indeterminacy of the type 0/0.

Page 234.

The value of digit X can be determined on the basis of the described
in chapter 3 methods of disclosing/expanding the
uncertainty/indeterminancy during the division into the basis/base.
With the formation/education of the quotient C could not have the
places one output/yield for the range, since number Ap_i lies/rests
in the range $[0, \mathscr{P})$ and basis/base p_i is its divider/denominator.
Therefore number C is obligated to lie/rest at the initial intervals
of range $[0, \mathscr{P})$.

Hence, if number A is first type critical number, then it is
obligated to coincide with number C, i.e.,
$$C = A,$$
$$X = \alpha_i.$$

But if number A is second type critical number, i.e., it
lies/rests at the latter/last intervals of numerical range, then
numbers A and C different in value $C \neq A$, and since in them coincide
digit in all bases/bases, besides digit on basis/base p_i, then is
obligated to occur the relationship/ratio

$$X \neq \alpha_i.$$

Further, if number A is first type critical number, then with
its multiplication on p_i cannot have places one output/yield beyond
the limits of numerical range.

However, for numbers of the second type of criticality with the multiplication on p_i occurs at least one output/yield beyond the limits of range. Therefore, if number A is first type critical number, then with its addition with itself itself p_i once occur the following equalities:

$$
\begin{aligned}
0 &= 2\Delta_A + \eta_{11} - \Delta_{2A} - \xi_{11} + \gamma_{11}, \\
0 &= \Delta_A + \Delta_{2A} + \eta_{21} - \Delta_{3A} - \xi_{21} + \gamma_{21}, \qquad (5.26) \\
0 &= \Delta_A + \Delta_{3A} + \eta_{31} - \Delta_{4A} - \xi_{31} + \gamma_{31}, \\
&\quad \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\
0 &= \Delta_A + \Delta_{(p_i-1)A} + \eta_{p_i-1,1} - \Delta_{Ap_i} - \xi_{p_i-1,1} + \gamma_{p_i-1,1}.
\end{aligned}
$$

Then, summarizing the right and left sides of equalities (5.26) and taking into account (5.23) and (5.25), we obtain

$$0 = p_i \Delta_A + \rho_2 - \Delta_{Ap_i} - \rho_1 + \rho_3$$

or

$$\Delta_A = \frac{\theta}{p_i}.$$

Thus, for first type critical numbers value θ it can take only the three values

$$\theta_1 = 0, \ \theta_2 = p_i, \ \theta_3 = -p_i.$$

Page 235.

Let us show now that for numbers of the second type of criticality value θ cannot have values, equal to θ_1, θ_2 and θ_3.

Let number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ with trace S_A be a number of

second type of criticality, i.e.,

$$\frac{\mathcal{P}}{p_n}(p_n - n + 2) < A < \mathcal{P},$$

but number $C = (\alpha_1, \alpha_2, \ldots, \alpha_i', \ldots, \alpha_n)$ with trace S_C is obtained by the step-by-step division of product Ap_i into basis/base p_i, i.e. it lies/rests at the region

$$\left[0, \ (n-1)\frac{\mathcal{P}}{p_n} \right).$$

According to the condition of theorem, basis/base p_n and p_i they satisfy the inequality

$$p_n \geqslant (n-1)\, p_i,$$

hence

$$\frac{\mathcal{P}}{p_i} > (n-1)\frac{\mathcal{P}}{p_n},$$

i.e. numbers C and A lie/rest at first and latter/last intervals $\frac{\mathcal{P}}{p_i}$ respectively.

In other words

$$A + \frac{\mathcal{P}}{p_i} = C,$$

whence

$$\alpha_i + K \equiv \alpha_i' \, (\mathrm{mod}\, p_i),$$
$$K = 1, 2, \ldots, p_i - 1.$$

Let us take for the certainty

$$\alpha_i + K < p_i,$$

i.e. we will count $\alpha_i' > \alpha_i$, and let us determine the difference ΔS in weights S_A and S_C, for it let us introduce minimum pseudo-orthogonal Mach number of the form

$$M = (0, 0, \ldots, K, \ldots, S_n^*).$$

Page 236.

It is obvious, that either

$$S_C = (S_A + S_k^*) \pmod{p_n}.$$

or

$$S_C = (S_A + S_k^* - 1) \pmod{p_n}$$

or, which is the same,

$$\Delta S = S_k^*$$

or

$$\Delta S = S_k^* - 1.$$

Then value θ_C for number C will differ from θ_A by $\Delta\theta$, i.e., is not less than to the number of transitions, which occur with addition S_k^* of very with itself p_i once. Difference $\Delta\theta$ cannot be equal to zero and cannot be multiple p_i, since with the addition of value $S_k^* < \dot{p}_n$ p_i of times a number of transitions cannot be equal to 0 or multiple p_i.

Thus, for numbers of the second type of criticality value θ cannot take the permissible for it values, equal to zero or multiple p_i. This composes the assertion of theorem, which consists in the fact that value θ determines the type of the criticality of an initial number.

Note. Under theorem conditions we learned to determine the
character of a number in the case, when it is first type critical. It
is possible to demonstrate symmetrical theorem, also, for second type
critical numbers. However, it seems that most simply in this case to
switch over to number $\mathscr{P} - A$, which is first type critical, to
determine its character $\Delta_{\mathscr{P}-A}$, and then to determine the character
of number A.

Theorem examined above about the type of criticality makes it
possible to determine the character of a critical number, if it is
known that after multiplication by basis/base p_i, the one satisfying
theorem conditions, product Ap_i loses criticality.

However, is feasible the case, when after multiplication by p_i
number Ap_i remains susceptible. In this case it is obvious that any
critical number can be converted into the noncritical by consecutive
multiplications by the bases/bases, which satisfy the conditions of
the nonintersection of rejection regions. In other words if is present
the system of bases/bases, then can be selected the sequence of the
bases/bases by multiplication by which any number can be brought out
from the region of criticality. There is no doubt that the selection
of the optimum sequence of multipliers is connected with the

selection of bases/bases themselves and it will be varied in each
specific case.

Page 237.

Let us note that on selected basis/base p_i is superimposed only
the limitation

$$p_i(n-1)+(n-3) \leqslant p_n$$

or if multiplier is selected multiple p_i, then

$$kp_i(n-1)+(n-3) \leqslant p_n,$$

whence

$$kp_i \leqslant \frac{p_n-n+3}{n-1}.$$

For the purpose of the reduction of the length of the process of
the definition of the character of a number it is desirable
multiplier value to choose as close as possible to the number

$$m_1 = \left[\frac{p_n-n+3}{n-1}\right] = \left[\frac{p_n+1}{n-1}\right]-1,$$

if p_n+2 is not multiple n-1, or as close as possible to the number

$$m_2 = \left[\frac{p_n+1}{n-1}\right],$$

if p_n+2 is multiple n-1.

As the first multiplier which subsequently we will designate
through v_1. it can be selected one of the bases/bases either the
value, multiple to any basis/base or the product of several
bases/bases.

The selection of one or the other value of multiplier v_1 is determined by the requirement of the greatest proximity from below to value m_1 or m_2. Let us assume that we succeeded in satisfying this condition, and we have

$$v_1 \approx \left[\frac{p_n+1}{n-1}\right] - 1,$$

but in this case product Av_1 remains in the critical range. Let us find the number of interval z_1, at which lies/rests small number $N_{min}^{(1)}$, such, that product $N_{min}^{(1)}v_1$ already leaves critical range $\left[0, (n-2)\frac{\mathcal{P}}{p_n}\right)$, i.e.

$$z_1 \frac{\mathcal{P}}{p_n} v_1 > (n-2)\frac{\mathcal{P}}{p_n},$$

whence

$$z_1 > \frac{n-2}{v_1}$$

or value z_1 can be defined as

$$z_1 = \left[\frac{n-2}{v_1}\right] + 1.$$

Page 238.

Let us find now this small number $N_{min}^{(1)}$ from interval $\left[0, z_1 \frac{\mathscr{P}}{p_n}\right)$

$$N_{min}^{(1)} v_1 \geqslant (n-2) \frac{\mathscr{P}}{p_n}$$

or, assuming that $n-2 \geqslant v_1$, we will obtain

$$N_{min}^{(1)} = \left[\frac{n-2}{v_1} \frac{\mathscr{P}}{p_n}\right] + 1.$$

It is obvious, following factor v_2, which is chosen for analogous reasons, it must satisfy the requirements so that the number $N_{min}^{(1)}$, multiplied by v_2, would not fall into second rejection region, i.e.,

$$N_{min}^{(1)} v_2 \leqslant (p_n - n + 3) \frac{\mathscr{P}}{p_n},$$

whence

$$v_2 < \frac{p_n - n + 3}{\left[\frac{n-2}{v_1} \cdot \frac{\mathscr{P}}{p_n}\right] + 1} \frac{\mathscr{P}}{p_n}.$$

Continuing this process, we with each step/pitch minuend is the section of the predicted determination of the initial number.

With each step/pitch increases the value of next factor, since the right boundary of noncritical zone increases, and the section of the predicted determination of an initial number is reduced.

Let us consider the use/application of the described method in

the more specific case. Let the number of bases n=9, and the largest base lie/rest within limits $31 < p_n < 63$. We will count $p_n = 47$.

1st step/pitch. First factor v_1 is defined, as is known, from the condition

$$v_1 (n-1) + (n-3) \leqslant p_n$$

or

$$v_1 \approx \frac{p_n - 6}{8} \approx 5.$$

Page 239.

The smallest number, which loses criticality with the multiplication on v_1, lies/rests at the interval with number z_1, defined from the condition

$$z_1 \geqslant \frac{n-2}{v_1}$$

or

$$z_1 = 2,$$

and the value of the smallest number is defined as

$$N_{min}^{(1)} = \left[\frac{7}{5} \frac{\mathscr{P}}{p_n} \right] + 1.$$

2nd step/pitch. Let us determine second factor v_2, on the basis of the fact that an initial number can be located not more to the right not first fourth of second interval, i.e.,

$$\left(\frac{\mathscr{P}}{p_n} + \frac{\mathscr{P}}{4 p_n} \right) v_2 \leqslant (p_n - n + 3) \frac{\mathscr{P}}{p_n} .$$

whence

$$v_2 \leqslant \frac{164}{5} \approx 32.$$

The smallest of the numbers, which lose criticality with the multiplication

$$N^{(2)}_{min} v_2 \geqslant (n-2) \frac{\mathscr{P}}{p_n}$$

or

$$N^{(2)}_{min} > \frac{7}{32} \frac{\mathscr{P}}{p_n},$$

lies/rests at first fourth or first interval. But in the case of second type criticality it is placed in latter/last fourth of latter/last interval. If an initial number remained susceptible, let us satisfy the third step/pitch.

3rd step/pitch. Let us determine the third factor of the condition

$$\frac{7}{32} \frac{\mathscr{P}}{p_n} v_3 < (p_n - n + 3) \frac{\mathscr{P}}{p_n},$$

whence

$$v_3 \leqslant 187.$$

The number, which did not lose criticality with the third multiplication, is located in the region whose right boundary is defined as

$$N^{(3)}_{min} v_3 \geqslant (n-2) \frac{\mathscr{P}}{p_n}$$

or

$$N^{(3)}_{min} > \frac{7}{187} \frac{\mathscr{P}}{p_n},$$

i.e., is located in a region less than $2 \frac{\mathscr{P}}{p_n^2}$.

Page 240.

4th step/pitch. If an initial number remained susceptible then
the fourth factor will be determined from the condition

$$\frac{7}{187} \cdot \frac{\mathscr{P}}{p_n} \cdot v_4 \leqslant (p_n - n + 3) \frac{\mathscr{P}}{p_n},$$

or

$$v_4 \leqslant 1095,$$

whence

$$N_{min}^{(4)} \geqslant \frac{7}{1095} \frac{\mathscr{P}}{p_n},$$

i.e., the number, which remains critical after the 4th step/pitch, is
located in a region less $\frac{\mathscr{P}}{4p_n^2}$.

The 5th step/pitch. Let us find the fifth factor

$$\frac{7}{1095} \frac{\mathscr{P}}{p_n} v_5 < (p_n - n + 3) \frac{\mathscr{P}}{p_n}, v_5 < 6413, N_{min}^{(5)} \geqslant \frac{7}{6413} \frac{\mathscr{P}}{p_n}.$$

It is not difficult to be convinced of the fact that the region of
the determination of an initial number after m steps/pitches is
reduced not less than v_1^m once where

$$v_1 \approx \left[\frac{p_n - n + 3}{n - 1} \right].$$

Intending sufficient to reduce the sizes/dimensions of the field
of uncertainty/indeterminancy to p_n, we will obtain that a number of
steps/pitches m will be determined from the condition

$$(n-2) \frac{\mathscr{P}}{p_n} \frac{1}{v_1^m} < p_n$$

or

$$(n-2) \frac{\mathscr{P}}{p_n^2} < v_1^m.$$

whence

$$m \geqslant \frac{\ln \left((n-2) \frac{\mathscr{P}}{p_n^2} \right)}{\ln v_1}.$$

With $n = 9$, $p_n = 47$, $\mathscr{P} = 10^k$

or

$$m \geqslant \frac{\ln 7 + k \ln 10 - 2 \ln 47!}{\ln 5}$$

$$m \geqslant 1,4k - 3,6,$$

i.e., for range $\mathscr{P} = 10^8 - 10^{10}$ we obtain m=8-10 multiplications.

Page 241.

Let us illustrate the described process based on specific example. Let be assigned the standardized/normalized system of the foundations:

$$p_1 = 3, \ p_2 = 7, \ p_3 = 11, \ p_4 = 13, \ p_5 = 17, \ p_6 = 19, \ p_7 = 23, \ p_8 = 25, \ p_9 = 47$$

with the range, P=26 213 412 225 and with the value of interval $\frac{\mathscr{P}}{p_n} = 557\ 732\ 175.$

Example. To find the set/dialing of factors for determining the character of a small number by method of the evaluation/estimate of intervals.

The first factor is determined from the condition

$$v_1 \leqslant \frac{p_n - n - 3}{n - 1} = \frac{41}{8} = 5.$$

i.e., as the first factor must be selected the near foundation $p_1 = 3$,

i.e., $v_1 = 3$. Then the number of the interval at which lies/rests the smallest number, which emerges with the multiplication beyond the limits of critical section $\left[0, (n-2)\frac{\mathscr{P}}{p_n}\right)$, is determined from the condition

$$z_1 > \frac{n-2}{v_1} = 3,$$

i.e., the number lies/rests not more to the right interval $\left[0, 3\frac{\mathscr{P}}{p_n}\right)$, or the smallest "noncritical" number exists

$$N_{min}^{(1)} = 3\frac{\mathscr{P}}{p_n}.$$

Hence the second factor is defined as

$$v_2 \leqslant \frac{p_n - n + 3}{3} = \frac{41}{3} = 13.6.$$

and as the second factor can be selected foundation $p_4 = 13$, i.e., $v_2 = 13$, and the smallest "noncritical" number will be

$$N_{min}^{(2)} > \frac{n-2}{v_2}\frac{\mathscr{P}}{p_n} = \frac{7}{13}\frac{\mathscr{P}}{p_n}.$$

We determine the third factor

$$v_3 \leqslant \frac{p_n - n + 3}{N_{min}^{(2)}}\frac{\mathscr{P}}{p_n} = \frac{533}{7} = 76.$$

As the third factor can be selected the product of foundations $p_1 = 3$, $p_8 = 25$, i.e., $v_3 = 75$. in this case the smallest noncritical number

$$N_{min}^{(3)} > \frac{n-3}{v_3}\frac{\mathscr{P}}{p_n} = \frac{6}{75}\frac{\mathscr{P}}{p_n}.$$

For the fourth factor we obtain

$$v_4 \leqslant \frac{42}{N_{min}^{(3)}}\frac{\mathscr{P}}{p_n} \quad 525.$$

Page 242.

As the fourth factor can be selected the product of foundations $p_1 = 3$, $p_2 = 7$, $p_8 = 25$, i.e., $v_4 = 525$.

Since in this case product we obtain at least with three zero numerals, the smallest number will be determined from the condition

$$N_{min}^{(4)} > \frac{n-4}{v_4} \frac{\mathscr{P}}{p_n} = \frac{5}{525} \frac{\mathscr{P}}{p_n} = \frac{1}{105} \frac{\mathscr{P}}{p_n}.$$

We assume that the fifth factor will be comprised of the product not less than of three foundations, then it is determined so

$$v_5 \leqslant \frac{p_n - n + 5}{N_{min}^{(4)}} \frac{\mathscr{P}}{p_n} = 4515.$$

As the fifth factor can be undertaken the product of the foundations: $p_3 = 11$, $p_5 = 17$, $p_7 = 23$, i.e., $v_5 = 4301$ and then the smallest number, which loses criticality with the multiplication, will be determined from the condition

$$N_{min}^{(5)} > \frac{n-4}{v_5} \frac{\mathscr{P}}{p_n} = \frac{5}{4301} \frac{\mathscr{P}}{p_n}.$$

Hence for the sixth factor

$$v_6 < \frac{p_n - n + 5}{N_{min}^{(5)}} \frac{\mathscr{P}}{p_n} = 36988.6,$$

which can be obtained as the product of foundations $p_1 = 3$, $p_3 = 11$, $p_7 = 23$, $p_9 = 47$, i.e., $v_6 = 35673$ and, therefore,

$$N_{min}^{(6)} > \frac{n-5}{v_6} \frac{\mathscr{P}}{p_n} = \frac{4}{35673} \cdot \frac{\mathscr{P}}{p_n}.$$

The seventh factor assumes the presence not less than four of the factors

$$v_7 < \frac{p_n - n + 6}{N_{min}^{(6)}} \frac{\mathscr{P}}{p_n} = 392403,$$

namely $p_1 = 3$, $p_3 = 11$, $p_6 = 13$, $p_8 = 17$, $p_9 = 47$, i.e., $v_7 = 350493$, whence

$$N_{min}^{(7)} > \frac{n-6}{v_7} \frac{\mathscr{P}}{p_n} = \frac{3}{350493} \frac{\mathscr{P}}{p_n}.$$

Further, the eighth factor

$$v_8 < \frac{p_n - n + 6}{N_{min}^{(7)}} \frac{\mathscr{P}}{p_n} = 4906902$$

can be represented as the product of foundations $p^2_1 = 9$, $p_6 = 19$, $p_7 = 23$, $p_8 = 25$, $p_9 = 47$, whence $v_8 = 4621275$. Then

$$V_{min}^{(8)} > \frac{n-7}{v_8} \frac{\mathscr{P}}{p_n} = \frac{2}{4621275} \frac{\mathscr{P}}{p_n}$$

or $V_{min}^{(8)} \approx 241$.

Page 243.

The ninth factor

$$v_9 < \frac{p_n - n + 8}{N_{min}^{(8)}} \frac{\mathscr{P}}{p_n} = 106289325$$

can be represented as the product of the foundations: $p^2_1 = 9$, $p_6 = 19$, $p^2_7 = 529$, $p_8 = 25$, $p_9 = 47$, whence $v_9 = 106289325$. Then

$$N_{min}^{(9)} > \frac{n-8}{v_9} \frac{\mathscr{P}}{p_n} = \frac{1}{106289325} \frac{\mathscr{P}}{p_n}$$

or $N_{min}^{(9)} \approx 6$.

In the case when after nine multiplications a number did not nevertheless lose criticality, it, as it was explained, cannot be more than 6. The contraction of range can be continued by multiplications, but it is considered by more advisable to compare it with one of the initial 6 numbers of the first interval. In the case of coincidence it is claimed that this number of the first s-band the known value of character, in the case of noncoincidence - an initial number is second type critical.

§5.4. Method of expanding the range.

Methods examined above of the definition of the minimum trace of
a number, number of the interval in which is arranged/located a
number, or the character of a number are characterized by systematic
simplicity, and their realization is possible both in the consecutive
and in the parallel performance.

In some of them is required the use of constants, which,
naturally, assumes the presence in the arithmetic unit of the
accumulator/storage of the constants of small amount of capacitance,
but working at the rate arithmetic unit.

The realization of these methods in the parallel performance,
naturally, is accompanied by a noticeable increase in the equipment,
and in the consecutive performance - by long time of the fulfillment
of process.

Let us now move on to the examination of some other methods of
determining the position characteristics of a number, in particular
the method of expanding the range.

Let be assigned the system of foundations $p_1, p_2, \ldots, p_n$ with range P, orthogonal by bases $B_1, B_2, \ldots, B_n$, whose weight respectively $m_1, m_2, \ldots, m_n$. Regarding

$$B_i = m_i \frac{\mathscr{P}}{p_i},$$
$$i = 1, 2, \ldots, n.$$

In this system is assigned number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Page 244.

Let us consider the now expanded system with which is connected additionally foundation p_{n+1}: $p_1, p_2, \ldots, p_n, p_{n+1}$, range of which orthogonal $\tilde{B}_1, \tilde{B}_2, \ldots, \tilde{B}_n, \tilde{B}_{n+1}$, and their weight $\tilde{m}_1, \tilde{m}_2, \ldots, \tilde{m}_n, \tilde{m}_{n+1}$, moreover

$$\tilde{B}_i = \tilde{m}_i \frac{p_{n+1}\mathscr{P}}{p_i},$$
$$i = 1, 2, \ldots, n+1.$$

Number A in this system will be represented in the form $A = (\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1})$. It is required on known numerals $\alpha_1, \alpha_2, \ldots, \alpha_n$ of the reference system of the foundations for determining the value of numeral α_{n+1} of number A in the expanded system of bases. It is logical that number A in the expanded system of bases will be a proper number, i.e., problem is reduced to the determination of the minimum trace of a number in the expanded system of foundations.

Let us write expressions for number A in essence and expanded

systems

$$A = \alpha_1 B_1 + \alpha_2 B_2 + \ldots + \alpha_n B_n - r_A \mathcal{P},$$
$$A = \alpha_1 \widetilde{B}_1 + \alpha_2 \widetilde{B}_2 + \ldots + \alpha_n \widetilde{B}_n + \alpha_{n+1} \widetilde{B}_{n+1} - \widetilde{r}_A p_{n+1} \mathcal{P}.$$

Equalizing the right sides of these expressions and determining from the obtained equation unknown numeral α_{n+1} for introduced foundation p_{n+1}, we will obtain

$$\alpha_{n+1} = \frac{1}{\widetilde{m}_{n+1}} \left\{ \alpha_1 \frac{m_1 - \widetilde{m}_1 p_{n+1}}{p_1} + \alpha_2 \frac{m_2 - \widetilde{m}_2 p_{n+1}}{p_2} + \ldots \right.$$
$$\left. \ldots + \alpha_n \frac{m_n - \widetilde{m}_n p_{n+1}}{p_n} - (r_A - \widetilde{r}_A p_{n+1}) \right\}$$

or

$$\widetilde{m}_{n+1} \alpha_{n+1} = \sum_{i=1}^{n} \alpha_i \frac{m_i - \widetilde{m}_i p_{n+1}}{p_i} - (r_A - \widetilde{r}_A p_{n+1}). \qquad (5.27)$$

For simplification in expression (5.27) let us demonstrate the following lemma.

Lemma 5.1. If is assigned the basic system of foundations $p_1, p_2, \ldots, p_n$ with range $\mathcal{P}$ and with weights of orthogonal bases of $m_1, m_2, \ldots, m_n$ and is assigned the expanded system of foundations $p_1, p_2, \ldots, p_n, p_{n+1}$, with range $P = p_{n+1} \mathcal{P}$ and weights of orthogonal bases $\widetilde{m}_1, \widetilde{m}_2, \ldots, \widetilde{m}_n, \widetilde{m}_{n+1}$, then value $m_i - \widetilde{m}_i p_{n+1}$ is multiple p_i.

Page 245.

Proof. In accordance with the determination of orthogonal base

we have

$$B_i = m_i \frac{\mathscr{P}}{p_i} = k_i p_i + 1,$$
$$i = 1, 2, \ldots, n,$$

either

$$m_i \mathscr{P} = k_i p_i^2 + p_i, \qquad (5.28)$$

and also

$$\tilde{B}_i = \tilde{m}_i \frac{p_{n+1} \mathscr{P}}{p_i} = \tilde{k}_i p_i + 1,$$
$$i = 1, 2, \ldots, n + 1,$$

or

$$\tilde{m}_i p_{n+1} \mathscr{P} = \tilde{k}_i p_i^2 + p_i, \qquad (5.29)$$

where $k_i, \tilde{k}_i$ – whole non-negative numbers. Subtracting (5.29) from (5.28), we will obtain

$$(m_i - \tilde{m}_i p_{n+1}) \mathscr{P} = (k_i - \tilde{k}_i) p_i^2. \qquad (5.30)$$

Since $\mathscr{P}$ contains p_i to the first degree, and in right side (5.30) it is contained factor p_i^2, then

$$m_i - \tilde{m}_i p_{n+1}$$

must contain by factor p_i, that also proves the confirmation of lemma.

Let us designate through λ_i the whole number:

$$\lambda_i = \frac{\tilde{m}_i p_{n+1} - m_i}{p_i}. \qquad (5.31)$$

Then (5.27) it is possible to rewrite in the form

$$\tilde{m}_{n+1} \alpha_{n+1} = - \sum_{i=1}^{n} \alpha_i \lambda_i - r_A + \tilde{r}_A p_{n+1}$$

or

$$\tilde{m}_{n+1} \alpha_{n+1} + r_A = - \sum_{i=1}^{n} \alpha_i \lambda_i + \tilde{r}_A p_{n+1}. \qquad (5.32)$$

Determination. Value

$$\sigma_A = \sum_{i=1}^{n} \alpha_i \lambda_i \qquad (5.33)$$

let us name the generalized sum of the numerals of number A or the simply generalized sum.

Page 246.

Let us represent value σ_A in the form

$$\sigma_A = k p_{n+1} - q,$$

where k and q - whole non-negative numbers, moreover

$$q < p_{n+1}.$$

Then (5.32) it seems in the form

$$\widetilde{m}_{n+1} \alpha_{n+1} + r_A = (\widetilde{r_A} - k) p_{n+1} + q \qquad (5.34)$$

or

$$\widetilde{m}_{n+1} \alpha_{n+1} + r_A \equiv q \,(\text{mod}\, p_{n+1}). \qquad (5.35)$$

Latter/last expression is the formula of the expansion of the range of numbers, transfer equation from the representation of a number in the basic K-band the representation of a number in the expanded range.

Let us consider now how by using the formula of expansion (5.35), it is possible to switch over to the representation of a

number in the expanded range.

As is known, for the assigned system of the foundations for, in particular for the basic system, there is one and only one set/dialing of minimum pseudo-orthogonal numbers.

On foundation p_1: $M_{\alpha_{11}}$, $M_{\alpha_{21}}$, ..., $M_{\alpha_{p_1-1,1}}$ with the ranks respectively r_{11}, r_{21}, ..., $r_{p_1-1,1}$.

On foundation p_2: $M_{\alpha_{12}}$, $M_{\alpha_{22}}$, ..., $M_{\alpha_{p_2-1,2}}$ with the ranks respectively r_{12}, r_{22}, ..., $r_{p_2-1,2}$

. . . .

On foundation p_{n-1}: $M_{\alpha_{1,n-1}}$, $M_{\alpha_{2,n-1}}$, ..., $M_{\alpha_{p_{n-1}-1,n-1}}$ with the ranks respectively $r_{1,n-1}$, $r_{2,n-1}$, ..., $r_{p_{n-1}-1,n-1}$. Constructing initial number $A = (\alpha_1, \alpha_2, ..., \alpha_{n-1}, \alpha_n)$ from minimum pseudo-orthogonal numbers, we will obtain the number

$$M_A = (\alpha_1, \alpha_2, ..., \alpha_{n-1}, S_A), \qquad (5.36)$$

whose rank according to the theorem about the rank of sum is defined as

$$r_{M_A} = \sum_{j=1}^{n-1} r_{\alpha_{ij}} - m_n \pi_{M_A}. \qquad (5.37)$$

Thus, in the basic system is designed number M_A, whose rank is accurately known, coinciding with the initial number A in all numerals, except numeral on the latter/last foundation.

Furthermore, about number M_A to us it is known that since it is obtained by addition $n-1$ of minimum pseudo-orthogonal numbers, then its greatest possible value

$$(M_A)_{max} = \frac{\mathscr{P}}{p_n} \left(n - 1 - \sum_{i=1}^{n-1} \frac{1}{p_i} \right) \qquad (5.38)$$

cannot be located more to the right of

the $(n-1)$ interval $\frac{\mathscr{P}}{p_n}$ in the basic system of foundations.

For the expanded system of foundations also there is an only system of minimum pseudo-orthogonal numbers. In particular, on foundation p_n minimum pseudo-orthogonal numbers take the form

$$\widetilde{M}_{a_n n} = (0, 0, \ldots, 0, \alpha_n, S_{n+1}^*),$$

i.e., they are numbers of form

$$\prod_{i=1}^{n-1} p_i = \frac{\mathscr{P}}{p_n},$$
$$\cdots \cdots \cdots \qquad (5.39)$$
$$j \prod_{i=1}^{n-1} p_i = j \frac{\mathscr{P}}{p_n}$$
$$\cdots \cdots \cdots \cdots \cdots$$
$$(p_n - 1) \prod_{i=1}^{n-1} p_i = (p_n - 1) \frac{\mathscr{P}}{p_n}.$$

We will subsequently each of these numbers accompany by index $k_{a_n n}$, which indicates its multiplicity relative to the smallest number.

After widening number M_A from (5.36) according to the formula

of expansion (5.35), using the value of rank (5.37), we will obtain

$$A' = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A, \alpha'_{n+1}). \qquad (5.40)$$

In the expanded system of foundations number A' differs from
unknown quantity A in terms of numerals of two latter/last
foundations.

Page 248.

Furthermore, since the expansion, without varying number value,
only defines its numeral on foundation p_{n+1}, then on the basis (5.38)
it is known that number A cannot be more than $(n-1)\frac{\mathscr{P}}{p_n}$,
arranged/located in the first interval of the expanded system $[0, \mathscr{P})$
it is a proper number.

Let us adjoin now to number A' to that determined (5.40),
similar of minimum pseudo-orthogoral numbers (5.39), which will
convert numeral on foundation p_n in α_n, the minimum number

$$\widetilde{M}_{\beta_n n} = (0, 0, \ldots, 0, \beta_n, \widetilde{S}^*_{\beta_n})$$

of multiplicity $k_{\beta_n n}$, where

$$\beta_n \equiv (\alpha_n - S_A)\,(\mathrm{mod}\, p_n).$$

As a result of addition we will obtain number $A^{(2)}$ of the form

$$A^{(2)} = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n, \alpha^{(2)}_{n+1}). \qquad (5.41)$$

In this case if had place $S_A = \alpha_n$, then the transformations of
number A' was not required even then

$$A' = A,$$

i.e., (5.40) is the unknown expansion of number A. Actually/really, all numerals of numbers A and A' in foundations $p_1, p_2, \ldots, p_n$ coincide, and in the value number A lies/rests at the first interval of the expanded range, i.e., it is the unknown proper number.

If did not occur situation $S_A = \alpha_n$, then we obtain number $A^{(2)}$. Moreover, if the multiplicity of number $\tilde{M}_{\beta_n n}$ was no more than $p_n - (n-1)$, i.e.

$$k_{\beta_n n} \leqslant p_n - (n-1),$$

then also it is possible to claim that obtained number $A^{(2)}$ is the unknown expansion of number A, since to number A', which does not exceed $(n-1)\dfrac{\mathcal{P}}{p_n}$, adjoined number $\tilde{M}_{\beta_n n}$, which does not exceed $(p_n - (n-1))\dfrac{\mathcal{P}}{p_n}$, the sum of these numbers does not exceed $\mathcal{P}$ - value of the first interval.

The indefinite situation appears, when

$$k_{\beta_n n} > p_n - (n-1).$$

Page 249.

In this case number $A^{(2)}$ can be placed either in the latter/last $(n-1)\dfrac{\mathcal{P}}{p_n}$ parts of the first interval $[0, \mathcal{P})$, or in the low-order $(n-2)\dfrac{\mathcal{P}}{p_n}$ parts of the second interval $[\mathcal{P}, 2\mathcal{P}]$, and then unknown is the

number

$$A^{(2)} = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n, (\alpha_{n+1}^{(2)} - 1)(\mathrm{mod}\, p_{n+1})).$$

Let us illustrate the method examined based on examples.

Let the basic system be assigned by the foundations:

$$p_1 = 5;\ p_2 = 7;\ p_3 = 11;\ p_4 = 13;\ p_5 = 17;\ p_6 = 19;\ p_7 = 23.$$

Let us compute for it the values of orthogonal bases and their weights:

$B_1 = 29\ 745\ 716$	$m_1 = 4$	$B_5 = 34\ 994\ 960$	$m_5 = 16$
$B_2 = 21\ 246\ 940$	$m_2 = 4$	$B_6 = 15\ 655\ 640$	$m_6 = 8$
$B_3 = 30\ 421\ 755$	$m_3 = 9$	$B_7 = 8\ 083\ 075$	$m_7 = 5$
$B_4 = 8\ 580\ 495$	$m_4 = 3$		

Range of system $\mathscr{P} = 37182145$.

Let us compute the values of minimum pseudo-orthogonal numbers with their ranks and multiplicities.

On foundation $p_1 = 5$:

$M_{11} = (1, 0, 0, 0, 0, 0, 1)$	$r_{11} = 1$	$k_{11} = 2$
$M_{21} = (2, 0, 0, 0, 0, 0, 2)$	$r_{21} = 1$	$k_{21} = 4$
$M_{31} = (3, 0, 0, 0, 0, 0, 12)$	$r_{31} = 5$	$k_{31} = 1$
$M_{41} = (4, 0, 0, 0, 0, 0, 13)$	$r_{41} = 6$	$k_{41} = 3$

On foundation $p_2 = 7$:

$$M_{12} = (0, 1, 0, 0, 0, 0, 2) \qquad r_{12} = 1 \qquad k_{12} = 1$$
$$M_{22} = (0, 2, 0, 0, 0, 0, 4) \qquad r_{22} = 2 \qquad k_{22} = 2$$
$$M_{32} = (0, 3, 0, 0, 0, 0, 6) \qquad r_{32} = 3 \qquad k_{32} = 3$$
$$M_{42} = (0, 4, 0, 0, 0, 0, 8) \qquad r_{42} = 4 \qquad k_{42} = 4$$
$$M_{52} = (0, 5, 0, 0, 0, 0, 10) \qquad r_{52} = 5 \qquad k_{52} = 5$$
$$M_{62} = (0, 6, 0, 0, 0, 0, 12) \qquad r_{62} = 6 \qquad k_{62} = 6$$

On foundation $p_3 = 11$:

$$M_{13} = (0, 0, 1, 0, 0, 0, 1) \qquad r_{13} = 1 \qquad k_{13} = 9$$
$$M_{23} = (0, 0, 2, 0, 0, 0, 11) \qquad r_{23} = 4 \qquad k_{23} = 7$$
$$M_{33} = (0, 0, 3, 0, 0, 0, 21) \qquad r_{33} = 7 \qquad k_{33} = 5$$
$$M_{43} = (0, 0, 4, 0, 0, 0, 8) \qquad r_{43} = 5 \qquad k_{43} = 3$$
$$M_{53} = (0, 0, 5, 0, 0, 0, 18) \qquad r_{53} = 8 \qquad k_{53} = 1$$
$$M_{63} = (0, 0, 6, 0, 0, 0, 19) \qquad r_{63} = 9 \qquad k_{63} = 10$$
$$M_{73} = (0, 0, 7, 0, 0, 0, 6) \qquad r_{73} = 7 \qquad k_{73} = 8$$
$$M_{83} = (0, 0, 8, 0, 0, 0, 16) \qquad r_{83} = 10 \qquad k_{83} = 6$$
$$M_{93} = (0, 0, 9, 0, 0, 0, 3) \qquad r_{93} = 8 \qquad k_{93} = 4$$
$$M_{10,3} = (0, 0, 10, 0, 0, 0, 13) \qquad r_{10,3} = 11 \qquad k_{103} = 2$$

Page 250.

On foundation $p_4 = 13$:

$$M_{14} = (0, 0, 0, 1, 0, 0, 22) \qquad r_{14} = 5 \qquad k_{14} = 4$$
$$M_{24} = (0, 0, 0, 2, 0, 0, 21) \qquad r_{24} = 5 \qquad k_{24} = 8$$
$$M_{34} = (0, 0, 0, 3, 0, 0, 20) \qquad r_{34} = 5 \qquad k_{34} = 12$$
$$M_{44} = (0, 0, 0, 4, 0, 0, 5) \qquad r_{44} = 2 \qquad k_{44} = 3$$
$$M_{54} = (0, 0, 0, 5, 0, 0, 4) \qquad r_{54} = 2 \qquad k_{54} = 7$$
$$M_{64} = (0, 0, 0, 6, 0, 0, 3) \qquad r_{64} = 2 \qquad k_{64} = 11$$
$$M_{74} = (0, 0, 0, 7, 0, 0, 11) \qquad r_{74} = 4 \qquad k_{74} = 2$$
$$M_{84} = (0, 0, 0, 8, 0, 0, 10) \qquad r_{84} = 4 \qquad k_{84} = 6$$
$$M_{94} = (0, 0, 0, 9, 0, 0, 9) \qquad r_{94} = 4 \qquad k_{94} = 10$$
$$M_{10,4} = (0, 0, 0, 10, 0, 0, 17) \qquad r_{10,4} = 6 \qquad k_{104} = 1$$
$$M_{11,4} = (0, 0, 0, 11, 0, 0, 16) \qquad r_{11,4} = 6 \qquad k_{114} = 5$$
$$M_{12,4} = (0, 0, 0, 12, 0, 0, 15) \qquad r_{12,4} = 6 \qquad k_{124} = 9$$

On foundation $p_5 = 17$:

$$M_{15} = (0, 0, 0, 0, 1, 0, 5) \qquad r_{15} = 2 \qquad k_{15} = 11$$
$$M_{25} = (0, 0, 0, 0, 2, 0, 19) \qquad r_{25} = 6 \qquad k_{25} = 5$$
$$M_{35} = (0, 0, 0, 0, 3, 0, 1) \qquad r_{35} = 3 \qquad k_{35} = 16$$
$$M_{45} = (0, 0, 0, 0, 4, 0, 15) \qquad r_{45} = 7 \qquad k_{45} = 10$$
$$M_{55} = (0, 0, 0, 0, 5, 0, 6) \qquad r_{55} = 6 \qquad k_{55} = 4$$
$$M_{65} = (0, 0, 0, 0, 6, 0, 11) \qquad r_{65} = 3 \qquad k_{65} = 5$$
$$M_{75} = (0, 0, 0, 0, 7, 0, 2) \qquad r_{75} = 7 \qquad k_{75} = 9$$
$$M_{85} = (0, 0, 0, 0, 8, 0, 16) \qquad r_{85} = 11 \qquad k_{85} = 3$$
$$M_{95} = (0, 0, 0, 0, 9, 0, 21) \qquad r_{95} = 13 \qquad k_{95} = 14$$
$$M_{10,5} = (0, 0, 0, 0, 10, 0, 12) \qquad r_{10,5} = 12 \qquad k_{105} = 8$$
$$M_{11,5} = (0, 0, 0, 0, 11, 0, 3) \qquad r_{11,5} = 11 \qquad k_{115} = 2$$
$$M_{12,5} = (0, 0, 0, 0, 12, 0, 8) \qquad r_{12,5} = 13 \qquad k_{125} = 13$$
$$M_{13,5} = (0, 0, 0, 0, 13, 0, 22) \qquad r_{13,5} = 17 \qquad k_{135} = 7$$
$$M_{14,5} = (0, 0, 0, 0, 14, 0, 13) \qquad r_{14,5} = 16 \qquad k_{145} = 1$$
$$M_{15,5} = (0, 0, 0, 0, 15, 0, 18) \qquad r_{15,5} = 18 \qquad k_{155} = 12$$
$$M_{16,5} = (0, 0, 0, 0, 16, 0, 9) \qquad r_{16,5} = 17 \qquad k_{165} = 6$$

On foundation $p_6 = 19$:

$$M_{16} = (0, 0, 0, 0, 0, 1, 12) \qquad r_{16} = 3 \qquad k_{16} = 13$$
$$M_{26} = (0, 0, 0, 0, 0, 2, 10) \qquad r_{26} = 3 \qquad k_{26} = 7$$
$$M_{36} = (0, 0, 0, 0, 0, 3, 8) \qquad r_{36} = 3 \qquad k_{36} = 1$$
$$M_{46} = (0, 0, 0, 0, 0, 4, 20) \qquad r_{46} = 6 \qquad k_{46} = 14$$
$$M_{56} = (0, 0, 0, 0, 0, 5, 18) \qquad r_{56} = 6 \qquad k_{56} = 8$$

$$M_{66} = (0, 0, 0, 0, 0, 6, 16) \qquad r_{66} = 6 \qquad k_{66} = 2$$
$$M_{76} = (0, 0, 0, 0, 0, 7, 5) \qquad r_{76} = 4 \qquad k_{76} = 15$$
$$M_{86} = (0, 0, 0, 0, 0, 8, 3) \qquad r_{86} = 4 \qquad k_{86} = 9$$
$$M_{96} = (0, 0, 0, 0, 0, 9, 1) \qquad r_{96} = 4 \qquad k_{96} = 3$$
$$M_{10,6} = (0, 0, 0, 0, 0, 10, 13) \qquad r_{10,6} = 7 \qquad k_{106} = 16$$
$$M_{11,6} = (0, 0, 0, 0, 0, 11, 11) \qquad r_{11,6} = 7 \qquad k_{116} = 10$$
$$M_{12,6} = (0, 0, 0, 0, 0, 12, 9) \qquad r_{12,6} = 7 \qquad k_{126} = 4$$
$$M_{13,6} = (0, 0, 0, 0, 0, 13, 21) \qquad r_{13,6} = 10 \qquad k_{136} = 17$$
$$M_{14,6} = (0, 0, 0, 0, 0, 14, 19) \qquad r_{14,6} = 10 \qquad k_{146} = 11$$
$$M_{15,6} = (0, 0, 0, 0, 0, 15, 17) \qquad r_{15,6} = 10 \qquad k_{156} = 5$$
$$M_{16,6} = (0, 0, 0, 0, 0, 16, 6) \qquad r_{16,6} = 8 \qquad k_{166} = 18$$
$$M_{17,6} = (0, 0, 0, 0, 0, 17, 4) \qquad r_{17,6} = 8 \qquad k_{176} = 12$$
$$M_{18,6} = (0, 0, 0, 0, 0, 18, 2) \qquad r_{18,6} = 8 \qquad k_{186} = 6$$

Page 251.

The expanded system cf foundations let us select in the form

$$p_1 = 5, \quad p_2 = 7, \quad p_3 = 11, \quad p_4 = 13, \quad p_5 = 17, \quad p_6 = 19, \quad p_7 = 23, \quad p_8 = 31.$$

with range $P = p_8 \mathcal{P} = 1152646495$ (its parameters they are given on page 268).

Values λ_i take the following values:

$$\lambda_1 = 24, \ \lambda_2 = 26, \ \lambda_3 = 2, \ \lambda_4 = 26; \ \lambda_5 = 10, \ \lambda_6 = 11, \ \lambda_7 = 20.$$

Example. To find the expanded representation of the number

$$A = (3, 3, 3, 3, 3, 3, 3).$$

Let us compute the trace of number A in the basic system

$$S_A = (12 + 6 + 21 + 20 + 1 + 8) \ (\text{mod } 23) = 22.$$

In this case occurred two transitions/junctions on foundation $p_7 = 23$, whence $\varkappa_A = 2$. Let us design number $M_A = (3, 3, 3, 3, 3, 3, 22)$, whose rank of (5.37) is equal to

$$r_{M_A} = 5 + 3 + 7 + 5 + 3 + 3 - 2 \times 5 = 16.$$

Let us present number M_A in the expanded range, for which let us compute the value of the generalized sum of the numerals

$$\sigma_A = 72 + 78 + 6 + 78 + 30 + 33 + 440 = 24 \cdot 31 - 7.$$

Whence

$$a_{n+1} - 16 = 7 \ (\text{mod } 31)$$

or $a_{n+1}' = 22$.

Thus, is obtained the expanded representation of the number

$$A' = (3, 3, 3, 3, 3, 3, 22, 22).$$

In order to switch over to the number, which has on foundation p_7 the numeral, equal to 3, it is necessary to adjoin the following minimum pseudo-orthogonal number of expanded range

$$\widetilde{M}_{67} = (0, 0, 0, 0, 0, 0, 4, 13).$$

which has multiplicity $k_{47}=20$.

Page 252.

In this case will be obtained number $A^{(2)}=(3, 3, 3, 3, 3, 3, 3, 4)$.
Here we clashed with the indefinite situation, since

$$k_{47} > p_7 - (n-1).$$

i.e., either number $A_1=(3, 3, 3, 3, 3, 3, 3, 4)$ lies/rests at the
first interval and is the unknown proper number, or it lies/rests at
the second interval, and the unknown proper number is $A_2=(3, 3, 3, 3, 3, 3, 3, 3)$. In this case, is examined the alternative set of
foundations, which includes the foundations, which correspond to all
possible errors.

Let the now following arithmetic operation be the multiplication
by the proper number $B=(3, 1, 1, 0, 11, 15, 8, 1)$: $(3, 3, 3, 3, 3, 3, 3, 3) \cdot (3, 1, 1, 0, 11, 15, 8, 1) = (4, 3, 3, 0, 16, 7, 1, 3)$. We
examine the obtained product $(A=(4, 3, 3, 0, 16, 7, 1)$ in the basic
system.

We find its trace

$$S_A = (13 + 6 + 21 + 9 + 5) \; (\text{mod } 23) = 8,$$

in this case $\pi_A = 2$.

We construct number $M_A = (4, 3, 3, 0, 16, 7, 8)$ and compute its rank

$$r_{M_A} = 6 + 3 + 7 + 17 + 4 - 2 \times 10 = 27.$$

We compute the generalized sum of the numerals

$$\sigma_A = 96 + 78 + 6 + 160 + 77 + 160 = 19 \times 31 - 12$$

and we translate number M_A into the expanded system

or
$$a'_{n+1} + 27 = 12$$
$$a'_{n+1} = 16,$$

i.e., obtain number $A' = (4, 3, 3, 0, 16, 7, 8, 16)$.

In order on foundation for p, obtaining numeral $a_n = 1$, it is necessary to number A' to adjoin a minimum pseudo-orthogonal number of expanded system

$$\widetilde{M}_{16,7} = (0, 0, 0, 0, 0, 0, 16, 18)$$

of multiplicity $k_{16,7} = 11$.

As a result we will obtain number $A^{(2)} = (4, 3, 3, 0, 16, 7, 1, 3)$. Since the condition

$$k_{16.7} < p_7 - (n - 1)$$

is satisfied, then it is possible to claim that number $A^{(2)}$ is proper, and therefore, is also proper the initial number $A = (3, 3, 3, 3, 3, 3,$

3, 3,).

§5.5. Method of reflection onto the end/lead cf the range.

In this method for number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n, X)$ it is necessary to find such value $X = \alpha_{n+1}$, at which A will be a proper number.

Page 253.

Let us multiply number A by certain factor q so as as a result to obtain a noncritical number. But since value of the X initial number is unknown, then it is necessary to examine the process of multiplication by the value, multiple p_{n+1}, in order to obtain in the product numeral on foundation p_{n+1}, identically equal to zero.

Hence, if we designate

$$q = \nu p_{n+1},$$

where ν - whole non-negative number, then factor ν it is expedient to choose as the product of the number of reasons for the purpose of the decrease cf the size of the zone of uncertainty/indeterminancy.

But then factor q can prove to be sufficiently high value and in the process cf multiplication will occur the transitions/junctions

through the numerical range P.

The number of transitions/junctions with the multiplication can
be evaluated on the basis of the following theorem.

Theorem 5.9. If in the standardized/normalized system of
foundations $p_1, p_2, \ldots, p_n, p_{n+1}$ is assigned number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1})$ with
trace S_A and character Δ_A and if with the multiplication of this
number by the factor

$$q = v p_{n+1},$$

where v - whole non-negative number, we obtain the product with
trace S_{np} and character Δ_{np}, then the number of transitions/junctions
through the numerical range P will be determined by the
relationship/ratio

$$\Omega = q\Delta_A - \Delta_{np} + v\alpha_{n+1} + \sum_{i=2}^{q} \gamma_{i-1,1} - \sum_{i=2}^{q} \xi_{i-1,1} \quad (5.42)$$

Proof. Let us present the multiplication of number A by factor q
as q of the additions of very in itself number A. For each addition
let us write out the criterion of the overfilling

$$\Omega_{1,1} = \Delta_A + \Delta_A + \eta_{1,1} + \gamma_{1,1} - \Delta_{2,1} - \xi_{1,1}$$
$$\Omega_{2,1} = \Delta_A + \Delta_{2A} + \eta_{2,1} + \gamma_{2,1} - \Delta_{3,1} - \xi_{2,1}$$
$$\cdots$$
$$\Omega_{q-1,1} = \Delta_A + \Delta_{(q-1)A} + \eta_{q-1,1} + \gamma_{q-1,1} - \Delta_{q,1} - \xi_{q-1,1}$$

After forming the left and right sides of these expressions, we will
obtain

$$\sum_{i=2}^{q} \Omega_{i-1, 1} = q\Delta_A - \Delta_{qA} + \sum_{i=2}^{q} \eta_{i-1, 1} + \sum_{i=2}^{q} \gamma_{i-1, 1} - \sum_{i=2}^{q} \xi_{i-1, 1}$$

Page 254.

Taking into account that $\Delta_{qA} = \Delta_{np}$ and

$$\sum_{i=2}^{q} \eta_{i-1, 1} = v\alpha_{n+1},$$

we will obtain that a number of transitions/junctions Ω through the range is determined in accordance with confirmation (5.42) of theorem.

Expression (5.42) can be simplified on the basis of the following theorem, which escape/ensues directly from the determination of the concept of the trace of a number.

Theorem 5.10. If in the system with foundations $p_1, p_2, \ldots p_n, p_{n+1}$ are assigned two numbers A_1 and A_2 with traces S_1 and S_2 respectively and their sum A_3 with trace S_3, then occurs the following relationship/ratio:

$$S_3 + \delta_{2, 1} - \gamma_{2, 1}p_{n+1} = S_1 + S_2 - \xi_{2, 1}p_{n+1}. \qquad (5.43)$$

Corollary 1. With the addition of number A whose trace S_A, very with themselves q of times occur the following equality:

$$\sum_{i=2}^{q} \gamma_{i-1, 1} - \sum_{i=2}^{q} \xi_{i-1, 1} = \frac{1}{p_{n+1}} \left(S_{np} + \sum_{i=2}^{q} \delta_{i-1, 1} \right) - vS_A. \quad (5.44)$$

Actually/really, let us designate the trace of number (i-1)A through S_{i-1}, in accordance with (5.43) we will obtain

$$S_i + \delta_{i-1,1} - \gamma_{i-1,1} p_{n+1} = S_{i-1} + S_A - p_{n+1}\xi_{i-1,1}.$$

Summarizing this expression on i with i=2, 3, ..., q, we will obtain

$$p_{n+1}\sum_{i=2}^{q}\gamma_{i-1,1} - p_{n+1}\sum_{i=2}^{q}\xi_{i-1,1} = S_{np} + \sum_{i=2}^{q}\delta_{i-1,1} - qS_A.$$

Whence it follows (5.44).

Corollary 2. In expression (5.44) left side is integral, that means the expression

$$S_{np} + \sum_{i=2}^{q}\delta_{i-1,1}$$

multiple p_{n+1}.

On the basis (5.44) the number of transitions/junctions through the range with the multiplication of number A by q will be defined as

$$\Omega = q\Delta_A - \Delta_{np} + v\alpha_{n+1} - vS_A + \frac{1}{p_{n+1}}\left(S_{np} + \sum_{i=2}^{q}\delta_{i-1,1}\right). \quad (5.45)$$

Page 255.

For the transformation of the obtained expression into the more

convenient for the realization let us consider some properties of minimum pseudo-orthogonal numbers.

A minimum pseudo-orthogonal number with numeral α_j on foundation p_j takes the form

$$M_{\alpha_j} = (0, 0, \ldots, 0, \alpha_j, 0, \ldots, S_{\alpha_j}^z). \qquad (5.46)$$

Since in number M_{α_j} all numerals zero, except numerals on foundations p_j and p_{n+1}, it must be multiple to value

$$\frac{P}{p_j p_{n+1}} = \frac{\mathscr{P}}{p_j}.$$

Let us consider numerical sequence

$$0, \frac{\mathscr{P}}{p_j}, 2\frac{\mathscr{P}}{p_j}, 3\frac{\mathscr{P}}{p_j}, \ldots, (p_j-1)\frac{\mathscr{P}}{p_j}. \qquad (5.47)$$

It is possible to claim that the numerical sequence in question is the complete set of minimum pseudo-orthogonal numbers on foundation p_j, in other words, in it are represented all values

$$\alpha_j = 0, 1, 2, \ldots, p_j - 1.$$

Actually/really, if on foundation p_j number $\frac{\mathscr{P}}{p_j}$ has a remainder/residue

$$\alpha' \equiv \frac{\mathscr{P}}{p_j} \pmod{p_j},$$

then the remaining members of sequence on foundation p_j have values

$$2\alpha' \pmod{p_j}, \ 3\alpha' \pmod{p_j}, \ \ldots, \ (p_j-1) \pmod{p_j}, \ 0 \pmod{p_j}.$$

Moreover any two numbers of this sequence are not congruent between themselves in modulus/module p_j. Let us prove this position from the opposite.

Let us assume that some two numbers of this sequence of multiplicity m and n are congruent with each other in modulus/module p_j, there obtains

$$m\alpha' \,(\mathrm{mod}\,p_j) \equiv n\alpha' \,(\mathrm{mod}\,p_j),$$

or

$$(m-n)\,\alpha' \equiv 0 \,(\mathrm{mod}\,p_j),$$

i.e.

$$(m-n)\,\alpha' = v p_j,$$

where v - whole non-negative number.

Page 256.

But latter/last equality cannot occur, since according to the condition

$$m < p_j,\; n < p_j,\; \alpha' < p_j$$

and none of these numbers has common divisors with p_j. Thus, any two numbers of sequence (5.47) are incomparable on modulus/module p_j.

These numbers in all p_j and possible values α_j also p_j. Hence numerical sequence (5.47) is the complete set of minimum pseudo-orthogonal numbers on foundation p_j.

As can easily be seen, the proved position is correct for the sequence, which begins from member $k_{\alpha_j} \frac{\mathscr{P}}{p_j}$.

Theorem 5.11. If in the system of foundations p_1, p_2, ..., p_n, p_{n+1} is assigned the minimum pseudo-orthogonal number

$$M_{\alpha_j j} = (0, 0, \ldots, 0, \alpha_j, 0, \ldots, 0, S^*_{\alpha_j})$$

of multiplicity $k_{\alpha_j j}$, then a quantity of incorrect pairs which forms numeral α_j with numerals 0, 1, 2, ..., $p_j - 1$, is equal to the multiplicity of minimum pseudo-orthogonal number $M_{\alpha_j j}$

$$\sum_{\beta_j=0}^{p_j-1} \delta_{\alpha_j \beta_j} = k_{\alpha_j j}. \qquad (5.48)$$

Proof. Actually/really, in the complete set of minimum pseudo-orthogonal numbers on foundation p_j are numbers of all possible multiplicities of value $\frac{\mathscr{P}}{p_j}$, namely

$$0, 1, 2, \ldots, p_j - 1.$$

Let us take an arbitrary number of this set/dialing of multiplicity $k_{\beta_j j}$

$$M_{\beta_j j} = (0, 0, \ldots, 0, \beta_j, 0, \ldots, 0, S^*_{\beta_j}).$$

Storing/adding up initial number $M_{\alpha_j j}$ with number $M_{\beta_j j}$ we will obtain

$$M_{\Sigma_j} = (0, 0, \ldots, 0, (\alpha_j - \beta_j) \pmod{p_j}, 0, \ldots, S_\Sigma) =$$
$$= (k_{\alpha_j j} - k_{\beta_j j}) \frac{\mathscr{P}}{p_j}.$$

where

$$S_\Sigma = (S^*_{\alpha_j} \div S^*_{\beta_j}) \pmod{p_{n+1}}.$$

Page 257.

If

$$k_{\alpha_j} + k_{\beta_j j} \geqslant p_j,$$

then

$$M_{\Sigma_j} \geqslant \mathcal{P},$$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\bullet$

i.e., the sum of such numbers is an incorrect number, and therefore, α_j and β_j compose incorrect pair. If

$$k_{\alpha_j} \div k_{\beta_j j} < p_j,$$

then

$$M_{\Sigma_j} < \mathcal{P},$$

i.e.

$$S^*_\Sigma = (S^*_{\alpha_j} \div S^*_{\beta_j}) \pmod{p_{n+1}}$$

and numerals α_j and β_j compose correct pair.

In other words, numeral α_j composes with the numeral of any number of the set/dialing of minimum pseudo-orthogonal numbers on modulus/module p_j incorrect pair in that and only in such a case, when the sum of their multiplicities is not less than the value of foundation p_j. But k_{α_j} satisfies this condition only with these numbers of the complete set whose multiplicities are

$$p_j - k_{\alpha_j}, \; p_j - k_{\alpha_j} \div 1, \; \ldots, \; p_j - 2, \; p_j - 1,$$

and such numbers in all k_{α_j}.

By this is proven confirmation (5.48) of theorem.

Theorem 5.12. If in the system of the foundations

$$p_1, \ p_2, \ \ldots, \ p_n, \ p_{n+1}$$

with range P number A

$$A = (\alpha_1, \ \alpha_2, \ \ldots, \ \alpha_j, \ \ldots, \ \alpha_n, \ \alpha_{n+1}),$$

it is multiplied by value q, where

$$q = \nu p_{n+1} = \frac{P}{p_j},$$

then a number of incorrect pairs, formed on foundation $p_\mu \neq p_j$, will be defined as

$$\delta_\mu = k_{\alpha_\mu \mu} \frac{P}{p_\mu p_j}, \qquad (5.49)$$

where through $k_{\alpha_\mu \mu}$ is designated the multiplicity of a minimum pseudo-orthogonal number with numeral α_μ on foundation p_μ.

Page 258.

Proof. Considering the multiplication of number A by value q as the addition of number A very with itself q of times, on the basis of theorem (5.11) it is possible to claim that $k_{\alpha_\mu \mu}$ is also a quantity of incorrect pairs which forms numeral α_l with the set/dialing of the numerals

$$0, \ 1, \ 2, \ 3, \ 4, \ \ldots, \ p_\mu - 2, \ p_\mu - 1.$$

But such sets/dialing with the multiplication of number A by j it will be in all

$$\frac{v p_{n+1}}{p_\mu} = \frac{P}{p_\mu p_j},$$

whence follows the confirmation of theorem.

Note. Into a quantity of incorrect pairs must not enter pairs, formable by digit of the initial number A with the appropriate numeral of product, since this pair in the addition does not participate.

However, when $p_\mu \neq p_j$ the corresponding numeral of product is equal identical to zero, and with any zero numeral is formed only correct pair.

Corollary 1. The sum of incorrect numerals $\delta_{\mu \neq j}$, formed on all foundations p_μ where $\mu = 1, 2, \ldots, n$ ($\mu \neq j$), is defined as

$$\delta_{\mu \neq j} = v p_{n+1} \sum_{\substack{\mu=1 \\ \mu \neq j}}^{n} \frac{k_{a_{\mu\mu}}}{p_\mu} = \frac{P}{p_j} \sum_{\substack{\mu=1 \\ \mu \neq j}}^{n} \frac{k_{a_{\mu\mu}}}{p_\mu}. \qquad (5.50)$$

Corollary 2. Expression (5.45) for the number of transitions/junctions through the range with the multiplication of number A on $v p_{n+1} = \frac{P}{p_j}$ can be represented in the form

$$\Omega = v p_{n+1} \Delta_A - \Delta_{np} + v \alpha_{n+1} - v S_A +$$
$$+ v \sum_{\substack{\mu=1 \\ \mu \neq j}}^{n} \frac{k_{a_{\mu\mu}}}{p_\mu} + \frac{1}{p_{n+1}} (S_{np} + \delta_j), \qquad (5.51)$$

where through δ_j is marked a number of incorrect pairs, formed on foundation p_j.

Corollary 3. A number of incorrect pairs δ, formed on foundations $p_1, p_2, \ldots, p_n$ with the multiplication of number A by the factor

$$\nu p_{n+1} = P,$$

will be defined as

$$\delta = \nu p_{n+1} \sum_{\mu=1}^{n} \frac{k_{\alpha\mu\mu}}{p_\mu} = P \sum_{\mu=1}^{n} \frac{k_{\alpha\mu\mu}}{p_\mu}. \qquad (5.52)$$

Page 259.

In this case expression for a quantity of overfillings takes the form

$$\Omega = \nu p_{n+1} \Delta_A + \nu \alpha_{n+1} - \nu S_A + \nu \sum_{\mu=1}^{n} \frac{k_{\alpha\mu\mu}}{p_\mu}, \qquad (5.53)$$

since with the multiplication by P we obtain the product, equal to zero, which has respectively $S_{np} = 0$ and $\Delta_{np} = 0$.

Somewhat more complicated matter proceeds with a number of incorrect pairs on foundation p_j, since value

$$\nu p_{n+1} = \frac{P}{n_j}$$

is not divided completely into p_j. Let us designate whole part of division νp_{n+1} into p_j through q_1, and the remainder/residue - through q_2. Then

$$\nu \cdot p_{n+1} = q_1 p_j + q_2.$$

Theorem 5.13. If in the system, calibrated on foundations p_j and p_{n+1}, the number

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_j, \ldots, \alpha_n, \alpha_{n+1})$$

is multiplied by value

$$\nu p_{n+1} = \frac{P}{p_j},$$

then significant digit in the product in foundation p_j coincides with the same in an initial number, and a number of incorrect pairs δ_j on foundation p_j with the multiplicity of minimum pseudo-orthogonal number k_{α_j} is determined by the formula

$$\delta_j = k_{\alpha_j} q_1, \qquad (5.54)$$

where

$$q_1 = \left[\frac{P}{p_j}\right].$$

Proof. According to theorem conditions has the place

$$\nu p_{n+1} = \frac{P}{p_j} = q_1 p_j + 1.$$

Therefore with the multiplication of numeral α_j of an initial number on νp_{n+1} we will obtain

$$\alpha_{np} \equiv (q_1 p_j + 1) \alpha_j \, (\bmod \, p_j) \equiv \alpha_j \, (\bmod \, p_j),$$

how is proven the first position of theorem.

Page 260.

A quantity of incorrect pairs on foundation p_j will be defined

as

$$\delta_j = k_{\alpha_j} q_1,$$

since the total quantity of components/terms/addends on foundation p_j is more than multiple k_{α_j} per unit, in other words, to a quantity of incorrect pairs between an initial number and a product.

However, this incorrect pair in δ_j be considered must not, since the result of product as the component/term/addend into total sum does not enter, that also proves the confirmation of theorem.

Corollary. Expression (5.51) taking into account (5.54) accepts the form

$$\Omega = \nu p_{n+1} \Delta_{\Lambda} - \Delta_{np} + \nu \alpha_{n+1} - \nu S_A +$$
$$+ \nu \sum_{\substack{\mu=1 \\ \mu \neq j}}^{n} \frac{k_{\alpha_{\mu\mu}}}{p_{\mu}} + \frac{1}{p_{n+1}} (S_{np} + k_{\alpha_j} q_1). \qquad (5.55)$$

Theorem 5.14. If in the system, calibrated on foundations p_j and p_{n+1}, the number

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n, \alpha_{n+1})$$

is multiplied by value

$$\nu p_{n+1} = \frac{P}{p_j},$$

then the trace of product S_{np} coincides with its minimum trace and is defined as

$$S_{np} = S_{np}^{\circ} = k_{\alpha_j} S^{\circ} \pmod{p_{n+1}}, \qquad (5.56)$$

where k_{α_j} - multiplicity of a minimum pseudo-orthogonal number with

numeral a_j on foundation p_j, and S^* - trace of a minimum pseudo-orthogonal number with the numeral on foundation p_j of the single multiplicity

$$S^* = \frac{P}{p_j p_{n+1}} (\mathrm{mod}\, p_{n+1}).$$

Proof. On the basis of the previous theorem it is known that significant digit in the product in foundation p_j coincides with the same in an initial number. The remaining numerals of product are equal to zero. Since the multiplication was produced to value

$$v p_{n+1} = \frac{P}{p_j}.$$

Page 261.

Therefore, the trace of product coincides with the trace of a minimum pseudo-orthogonal number with numeral a_j on foundation p_j, which according to the condition have a multiplicity $k_{z_j j}$. But then is correct relationship/ratio (5.56), which is the confirmation of theorem.

Theorem 5.15. In the system, calibrated on foundations p_j and p_{n+1} occurs the relationship/ratio

$$q_1 = x p_{n+1} + p_{n+1} - S^*, \qquad (5.57)$$

where q_1 is determined from expression $\frac{P}{p_j} = q_1 p_j - 1$; x - a whole non-negative number; S^* - trace of a minimum pseudo-orthogonal number with the numeral on foundation p_j of single multiplicity.

Proof. Value q_1, determined by expression (5.57), let us present in the form

$$q_1 = x p_{n+1} - \rho,$$

where x - whole non-negative number, while $\rho < p_{n+1}$. Then

or

$$\frac{P}{p_j} = x p_j p_{n+1} - \rho p_j + 1$$

$$p_j \rho + 1 \equiv 0 \ (\mathrm{mod}\ p_{n+1}). \qquad (5.58)$$

Under the conditions of theorem latter/last comparison has unique solution.

Let us write expression for the minimum pseudo-orthogonal number of single multiplicity

$$\frac{P}{p_j p_{n+1}} = (0, 0, \ldots, \alpha_j^{(1)}, 0, \ldots, S^\bullet) = \alpha_j^{(1)} \frac{P}{p_j} + S^\bullet \frac{P}{p_{n+1}} - P.$$

From this expression it follows that

or

$$p_j p_{n+1} - S^\bullet p_j + 1 = \alpha_j^{(1)} p_{n+1}$$

$$p_j (p_{n+1} - S^\bullet) + 1 \equiv 0 \ (\mathrm{mod}\ p_{n+1}).$$

Then

$$\rho = p_{n+1} - S^\bullet$$

it is the solution of comparison (5.58), which proves confirmation (5.57) of theorem.

Corollary 1. Value $S_{np} + k_{\alpha_j} q_1$ can be represented in the form

$$S_{np} + k_{\alpha_j} q_1 = x k_{\alpha_j} p_{n+1} - l_j p_{n+1} - p_{n+1}. \qquad (5.59)$$

where l_j is the integer part of the expression

$$l_j = \left[\frac{p_{n+1} - S^\bullet}{p_{n+1}} k_{\alpha_j} \right]. \qquad (5.60)$$

Page 262.

Actually/really, on the basis (5.56) and (5.57) value $S_{np} + k_{\alpha_j j} q_1$ can be represented as

$$S_{np} + k_{\alpha_j j} q_1 = k_{\alpha_j j} S^* (\mathrm{mod}\, p_{n+1}) + \varkappa p_{n+1} k_{\alpha_j j} + (p_{n+1} - S^*) k_{\alpha_j j}$$

or, taking into account (5.60),

$$S_{np} + k_{\alpha_j j} q_1 = \varkappa k_{\alpha_j j} p_{n+1} + l_j p_{n+1} + k_{\alpha_j j} S^* (\mathrm{mod}\, p_{n+1}) + $$
$$+ k_{\alpha_j j} (p_{n+1} - S^*) (\mathrm{mod}\, p_{n+1}),$$

whence

$$S_{np} + k_{\alpha_j j} q_1 = \varkappa k_{\alpha_j j} p_{n+1} + l_j p_{n+1} + p_{n+1}.$$

Corollary 2. On the basis of theorems presented above, expression (5.55) accepts the following form:

$$\Omega = \nu p_{n+1} \Delta_A - \Delta_{np} + \nu \alpha_{n+1} - \nu S_A + $$
$$+ \nu \sum_{\substack{\mu=1 \\ \mu \neq j}}^{n} \frac{k_{\alpha_{\mu\mu}}}{p_\mu} + \varkappa k_{\alpha_j j} + l_j + 1$$

or

$$\Omega = \nu(p_{n+1} \Delta_A + \alpha_{n+1} - S_A) + \nu \sum_{\substack{\mu=1 \\ \mu \neq j}}^{n} \frac{k_{\alpha_{\mu\mu}}}{p_\mu} + \varkappa k_{\alpha_j j} + l_j + 1 - \Delta_{np}.$$

$$(5.61)$$

Let us find this value of digit α_{n+1}, with which number A arranged/located in the first interval, i.e., it is correct. In this case a maximum number of transitions through range P is determined by

a number of transitions with the multiplication of the greatest number of first interval by multiplier νp_{n+1}, namely:

$$\left(\frac{r}{p_{n+1}} - 1\right)\nu p_{n+1} = \nu P - \frac{r}{p_j},$$

i.e. value Ω cannot take the values, which exceed value $\nu - 1$ for the numbers, arranged/located in the first interval.

Further, if a number is arranged/located in the first interval, then $\alpha_{n+1} = S_A^*$ and the character of initial number Δ_A can take only values of 0 and -1, moreover the situation when $\Delta_A = -1$, can occur, if zero numerical range fall into interval $(S_A - (n-2), S_A)$.

Page 263.

Let us introduce the parameter θ, defined as

$$\theta = \begin{cases} 1, & \text{если } \alpha_j = 0, \\ 0, & \text{если } \alpha_j \neq 0, \end{cases} \qquad (5.62)$$

Key: (1). if.

then

$$\theta = 1 - \Delta_{\text{пр}}. \qquad (5.63)$$

Actually/really, if $\alpha_j = 0$, the product consists of some zero ligits for which $\Delta_{\text{пр}} = 0$, and then $\theta = 1$.

But if $\alpha_j \neq 0$, then the trace of the product

$$S_{np} \neq 0,$$

and since digit on basis/base p_{n+1} in the product is identically equal
to zero, then regarding the character we obtain

$$\Delta_{np} = 1, \ \theta = 0.$$

Theorem 5.1p. (θ the criterion of the correctness of a number).
If in the system, calibrated on bases/bases p_j and p_{n+1}, the number

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_j, \ldots, \alpha_n, \alpha_{n+1})$$

with trace S_A and character Δ_A, then the criterion of the correctness
of the preset number is preset is satisfaction of the condition

$$p_{n+1}\Delta_A + \alpha_{n+1} - S_A + t = 0, \qquad (5.64)$$

where t - whole non-negative number, determined from the condition

$$\nu \sum_{\substack{\mu=1 \\ \mu \neq j}}^{n} \frac{k_{\alpha_{\mu\mu}}}{p_\mu} + x k_{\alpha,j} + l_j + \theta = t\nu + r \overset{(1)}{\text{при}} \nu = \frac{P}{p_j p_{n+1}} \quad (5.65)$$

Key: (1). with.

or from the condition

$$\nu \sum_{\substack{\mu=1 \\ \mu \neq j}}^{n} \frac{k_{\alpha_{\mu\mu}}}{p_\mu} = t\nu + r \overset{(1)}{\text{при}} \ p_{n+1}\nu = P. \qquad (5.66)$$

Key: (1). with.

where r - the whole non-negative number

$$r < \nu.$$

Proof. After introducing designations in accordance with (5.65) or (5.66), we can (5.53) and (5.61) register in the form

$$\Omega = v(p_{n+1}\Delta_A + \alpha_{n+1} - S_A + t) + r.$$

Page 264.

but value Ω cannot exceed value $v-1$, whence follows the assertion of theorem.

Corollary 1. The unknown value of digit α_{n+1}, with which number A is correct, is determined by the formula

$$\alpha_{n+1} = (S_A - t)(\mathrm{mod}\, p_{n+1}). \qquad (5.67)$$

Actually/really, if $S_A - t \geqslant 0$, then from (5.64) it follows that

$$p_{n+1}\Delta_A + \alpha_{n+1} \geqslant 0.$$

Since

$$p_{n+1} > \alpha_{n+1} \geqslant 0.$$

that this case can have place only under condition $\Delta_A = 0$, $\alpha_{n+1} = S_A - t$, which satisfies (5.67). But if $S_A - t < 0$, then $p_{n+1}\Delta_A - \alpha_{n+1} < 0$. whence, since $\alpha_{n+1} \geqslant 0$, can occur only case $\Delta_A = -1$ and $\alpha_{n+1} = p_{n+1} + S_A - t$, i.e. (5.67) is correct in this case.

Corollary 2. On the basis of the aforesaid, we obtain the following determination of the value of the character of the initial number A:

$$\Delta_A = \begin{cases} 0, & \text{если } S_A - t \geqslant 0, \\ 1, & \text{если } S_A - t < 0. \end{cases} \qquad (5.68)$$

Key: (1). if.

Let us consider the determination of value t with the multiplication on $q = v p_{n+1} = P$. In this case expression (5.66) can be represented in the form

$$tv + r = k_1 \frac{\mathscr{P}}{p_1} + k_2 \frac{\mathscr{P}}{p_2} + \ldots + k_n \frac{\mathscr{P}}{p_n}, \qquad (5.69)$$

where $\mathscr{P} = \frac{P}{p_{n+1}} = v$, which is equivalent to transition from the system of bases/bases $p_1, p_2, \ldots, p_n, p_{n+1}$ with range $P = \prod_{i=1}^{n+1} p_i = p_{n+1} \mathscr{P}$ to the abbreviated/reduced system of bases/bases $p_1, p_2, \ldots, p_n$ with range $v = \mathscr{P}$.

Page 265.

Value t in this system is nothing else but a number of transitions through the range of system with the addition of the members of the right side of expression (5.69), and k_i - whole non-negative numbers, which satisfy the expression

$$k_i \widetilde{a}_i \,(\mathrm{mod}\, p_i) = \alpha_i,$$
$$i = 1, 2, \ldots, n,$$

where α_i - digit of the number being investigated on basis/base p_i, and

$$\widetilde{\alpha}_i = \frac{P}{p_i p_{n+1}} \,(\mathrm{mod}\, p_i). \quad i = 1, 2, \ldots, n,$$

or, which is the same thing,

$$k_i \frac{v}{p_i} = x_{1i} p_i + \alpha_i, \qquad (5.70)$$

where x_{1i} - whole non-negative number.

If we through m_i designate the weights of orthogonal bases in the abbreviated/reduced system of bases/bases, then occurs the equality

$$m_i \frac{v}{p_i} = x_{2i} p_i + 1,$$

where x_{2i} - whole non-negative numbers.

After multiplying both parts of this equality on α_i

$$\alpha_i m_i \frac{v}{p_i} = x_{2i} \alpha_i p_i + \alpha_i$$

and after comparing with (5.70), we will obtain

$$k_i \equiv \alpha_i m_i \,(\mathrm{mod}\, p_i),$$

whence

$$k_i \frac{v}{p_i} = \alpha_i m_i \frac{v}{p_i} - \left[\frac{\alpha_i m_i}{p_i} \right] v$$

or

$$k_i \frac{v}{p_i} = \alpha_i m_i \frac{v}{p_i} - r_i v,$$

where

$$r_i = \left[\frac{\alpha_i m_i}{p_i} \right].$$

Now expression (5.69) can be represented in the form

$$tv + r = \sum_{i=1}^{n} \alpha_i m_i \frac{v}{p_i} - v \sum_{i=1}^{n} r_i. \qquad (5.71)$$

An initial number in the abbreviated/reduced system takes form $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Let us designate its trace through S_A. The rank of

number A' usually is accurately unknown, since during the composition
of number A' from the minimum pseudo-orthogonal components could
occur unfixed overflow.

Page 266.

But is always known the true rank of number $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S'_A)$,   since
during engineering of this number of the minimum numbers could not
have places one disregarded transition for the range.

Let us designate the true rank of this number through $r_{\text{ист}}$.

Then

$$(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S'_A) = \sum_{i=1}^{n-1} \alpha_i m_i \frac{\nu}{p_i} + S'_A m_n \frac{\nu}{p_n} - r_{\text{ист}} \nu.$$

Whence

$$\sum_{i=1}^{n-1} \alpha_i m_i \frac{\nu}{p_i} = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S'_A) + r_{\text{ист}} \nu - S'_A m_n \frac{\nu}{p_n},$$

and, after substituting this expression in (5.71), we will obtain

$$t\nu + r = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S'_A) + r_{\text{ист}} \nu - $$

$$- S'_A m_n \frac{\nu}{p_n} + \alpha_n m_n \frac{\nu}{p_n} - \nu \sum_{i=1}^{n} r_i$$

or

$$tv + r = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A') + ((\alpha_n - S_A') m_n) (\mathrm{mod}\, p_n) \frac{v}{p_n} +$$

$$\div v \left(r_{\text{ист}} - \sum_{i=1}^{n} r_i + \left[\frac{\alpha_n - S_A'}{p_n} m_n \right] \right),$$

whence, if $\alpha_n = S_A'$, follows that

$$t = r_{\text{ист}} - \sum_{i=1}^{n} r_i.$$

When $\alpha_n > S_A'$ are possible two cases:

a) $^{(1)}$если $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A') + ((\alpha_n - S_A') m_n (\mathrm{mod}\, p_n) \times$

$\times \frac{v}{p_n} < v,$ $^{(2)}$то $t = r_{\text{ист}} - \sum_{i=1}^{n} r_i + \left[\frac{\alpha_n - S_A'}{p_n} m_n \right],$

б) если $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A') + ((\alpha_n - S_A') m_n) (\mathrm{mod}\, p_n) \times$

$\times \frac{v}{p_n} \geqslant v,$ то $t = r_{\text{ист}} - \sum_{i=1}^{n} r_i + \left[\frac{\alpha_n - S_A'}{p_n} m_n \right] + 1.$

Key: (1). if. (2). then.

Page 267.

When $\alpha_n < S_A'$ are also possible two cases:

a) если $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A') \geqslant ((S_A' - \alpha_n) m_n) (\mathrm{mod}\, p_n) \frac{v}{p_n},$

Key: (1). if.

then

$$t = r_{\text{ист}} - \sum_{i=1}^{n} r_i + \left[\frac{\alpha_n - S_A'}{p_n} m_n \right],$$

б) $^{(1)}$если $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A') < ((S_A - \alpha_n) m_n) (\mathrm{mod}\, p_n) \frac{v}{p_n},$

Key: (1). if.

then

$$t = r_{\text{ист}} - \sum_{i=1}^{n} r_i + \left[\frac{\alpha_n - S_A'}{p_n} m_n \right] - 1.$$

Thus, is proved the following theorem.

Theorem 5.17. If in the standardized/normalized system of the bases/bases

$$p_1, p_2, \ldots, p_n, p_{n+1}$$

is preset number A with trace S_A and with digits $\alpha_1, \alpha_2, \ldots, \alpha_n$ on bases/bases $p_1, p_2, \ldots, p_n$ respectively, then digit α_{n+1}, with which number A is correct, is defined from the condition

$$\alpha_{n+1} = \left(S_A - r_{\text{ист}} + \sum_{i=1}^{n} r_i - \left[\frac{\alpha_n - S_A'}{p_n} m_n \right] + \Delta_1 \right) (\text{mod } p_n),$$

$$(5.72)$$

where $r_{\text{ист}}$ – true rank of number $M_{A'}$; S_A' – the trace of number A';
$M_{A'} = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A')$ and

$$r_i = \left[\frac{\alpha_i m_i}{p_i} \right]$$

in the abbreviated/reduced system of bases/bases $p_1, p_2, \ldots, p_n$, of rank Δ_1 is defined as

$$
\Delta_1 =
\begin{cases}
1, \text{ если при } \alpha_n < S_A' \text{ имеет место} \\
(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A') < ((S_A' - \alpha_n) m_n) \times \\
\qquad\qquad\qquad \times (\bmod\, p_n) \dfrac{\nu}{p_n}\,. \\
-1, \text{ если при } \alpha_n > S_A \text{ имеет место} \qquad (5.73) \\
(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A') + ((\alpha_n - S_A') m_n) \times \\
\qquad\qquad\qquad \times (\bmod\, p_n) \dfrac{\nu}{p_n} > \nu, \\
0, \text{ в остальных случаях.}
\end{cases}
$$

Key: (1). if with. (2). has place. (3). in remaining cases.

Page 268.

Note. Since $M_{A'}$ - number, comprised by addition $(n-1)$ of minimum pseudo-orthogonal numbers, then occurs the following limitation to its value:

$$
M_{A'} = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A') < (n-1)\frac{\nu}{p_n}\,.
$$

This limitation in the majority of the cases allows on (5.73) to accurately determine value of Δ_1. However, are possible the critical cases, when α_{n+1} is determined with an accuracy to unity, if $\alpha_n < S_A'$ and in this case

$$
(S_A' - \alpha_n) m_n (\bmod\, p_n) < n - 1,
$$

or if $\alpha_n > S_A'$ and in this case

$$
(\alpha_n - S_A') m_n (\bmod\, p_n) > p_n - (n-1).
$$

Let us illustrate, based on examples, the determination of the minimum trace of a number by method of the multiplication of an

initial number to value P. Let us consider the reference system of
numeration with bases/bases $p_1=5$; $p_2=7$; $p_3=11$; $p_4=13$; $p_5=17$; $p_6=19$;
$p_7=23$; $p_8=31$, with range $P=1\ 152\ 646\ 495$ and orthogonal bases with
their weights

$$B_1 = 922\ 117\ 196 \quad m_1 = 4;$$
$$B_2 = 987\ 982\ 710 \quad m_2 = 6;$$
$$B_3 = 104\ 786\ 045 \quad m_3 = 1;$$
$$B_4 = 975\ 316\ 265 \quad m_4 = 11;$$
$$B_5 = 406\ 816\ 410 \quad m_5 = 6;$$
$$B_6 = 424\ 659\ 235 \quad m_6 = 7$$
$$B_7 = 751\ 725\ 975 \quad m_7 = 15;$$
$$B_8 = \ \ 37\ 182\ 145 \quad m_8 = 1$$

Let us compute minimum pseudo-orthogonal numbers with their
multiplicities.

On basis/base $p_1=5$:

$$M_{11} = (1,\ 0,\ 0,\ 0\ ,\ 0,\ 0,\ 0,\ 7) \quad k_{11} = 4$$
$$M_{21} = (2,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 13) \quad k_{21} = 3$$
$$M_{31} = (3,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 19) \quad k_{31} = 2$$
$$M_{41} = (4,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 25) \quad k_{41} = 1$$

On basis/base $p_2=7$

$$M_{12} = (0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 5) \quad k_{12} = 4$$
$$M_{22} = (0,\ 2,\ 0,\ 0,\ 0,\ 0,\ 0,\ 9) \quad k_{22} = 1$$
$$M_{32} = (0,\ 3,\ 0,\ 0,\ 0,\ 0,\ 0,\ 14) \quad k_{32} = 5$$
$$M_{42} = (0,\ 4,\ 0,\ 0,\ 0,\ 0,\ 0,\ 18) \quad k_{42} = 2$$
$$M_{52} = (0,\ 5,\ 0,\ 0,\ 0,\ 0,\ 0,\ 23) \quad k_{52} = 6$$
$$M_{62} = (0,\ 6,\ 0,\ 0,\ 0,\ 0,\ 0,\ 27) \quad k_{62} = 3$$

Page 269.

On basis/base $p_3=11$:

$$M_{13} = (0, 0, 1, 0, 0, 0, 0, 29) \qquad k_{13} = 9$$
$$M_{23} = (0, 0, 2, 0, 0, 0, 0, 26) \qquad k_{23} = 7$$
$$M_{33} = (0, 0, 3, 0, 0, 0, 0, 23) \qquad k_{33} = 5$$
$$M_{43} = (0, 0, 4, 0, 0, 0, 0, 20) \qquad k_{43} = 3$$
$$M_{53} = (0, 0, 5, 0, 0, 0, 0, 17) \qquad k_{53} = 1$$
$$M_{63} = (0, 0, 6, 0, 0, 0, 0, 15) \qquad k_{63} = 10$$
$$M_{73} = (0, 0, 7, 0, 0, 0, 0, 12) \qquad k_{73} = 8$$
$$M_{83} = (0, 0, 8, 0, 0, 0, 0, 9) \qquad k_{83} = 6$$
$$M_{93} = (0, 0, 9, 0, 0, 0, 0, 6) \qquad k_{93} = 4$$
$$M_{10,3} = (0, 0, 10, 0, 0, 0, 0, 3) \qquad k_{10,3} = 2$$

On basis/base $p_4 = 13$:

$$M_{14} = (0, 0, 0, 1, 0, 0, 0, 5) \qquad k_{14} = 3$$
$$M_{24} = (0, 0, 0, 2, 0, 0, 0, 10) \qquad k_{24} = 6$$
$$M_{34} = (0, 0, 0, 3, 0, 0, 0, 15) \qquad k_{34} = 9$$
$$M_{44} = (0, 0, 0, 4, 0, 0, 0, 20) \qquad k_{44} = 12$$
$$M_{54} = (0, 0, 0, 5, 0, 0, 0, 24) \qquad k_{54} = 2$$
$$M_{64} = (0, 0, 0, 6, 0, 0, 0, 29) \qquad k_{64} = 5$$
$$M_{74} = (0, 0, 0, 7, 0, 0, 0, 3) \qquad k_{74} = 8$$
$$M_{84} = (0, 0, 0, 8, 0, 0, 0, 8) \qquad k_{84} = 11$$
$$M_{94} = (0, 0, 0, 9, 0, 0, 0, 12) \qquad k_{94} = 1$$
$$M_{10,4} = (0, 0, 0, 10, 0, 0, 0, 17) \qquad k_{10,4} = 4$$
$$M_{11,4} = (0, 0, 0, 11, 0, 0, 0, 22) \qquad k_{11,4} = 7$$
$$M_{12,4} = (0, 0, 0, 12, 0, 0, 0, 27) \qquad k_{12,4} = 10$$

On basis/base $p_5 = 17$:

$$M_{15} = (0, 0, 0, 0, 1, 0, 0, 21) \qquad k_{15} = 16$$
$$M_{25} = (0, 0, 0, 0, 2, 0, 0, 10) \qquad k_{25} = 15$$
$$M_{35} = (0, 0, 0, 0, 3, 0, 0, 30) \qquad k_{35} = 14$$
$$M_{45} = (0, 0, 0, 0, 4, 0, 0, 19) \qquad k_{45} = 13$$
$$M_{55} = (0, 0, 0, 0, 5, 0, 0, 8) \qquad k_{55} = 12$$
$$M_{65} = (0, 0, 0, 0, 6, 0, 0, 28) \qquad k_{65} = 11$$
$$M_{75} = (0, 0, 0, 0, 7, 0, 0, 17) \qquad k_{75} = 10$$
$$M_{85} = (0, 0, 0, 0, 8, 0, 0, 6) \qquad k_{85} = 9$$
$$M_{95} = (0, 0, 0, 0, 9, 0, 0, 26) \qquad k_{95} = 8$$
$$M_{10,5} = (0, 0, 0, 0, 10, 0, 0, 15) \qquad k_{10,5} = 7$$
$$M_{11,5} = (0, 0, 0, 0, 11, 0, 0, 4) \qquad k_{11,5} = 6$$

$$M_{12,5} = (0, 0, 0, 0, 12, 0, 0, 24) \quad k_{12,5} = 5$$
$$M_{13,5} = (0, 0, 0, 0, 13, 0, 0, 13) \quad k_{13,5} = 4$$
$$M_{14,5} = (0, 0, 0, 0, 14, 0, 0, 2) \quad k_{14,5} = 3$$
$$M_{15,5} = (0, 0, 0, 0, 15, 0, 0, 22) \quad k_{15,5} = 2$$
$$M_{16,5} = (0, 0, 0, 0, 16, 0, 0, 11) \quad k_{16,5} = 1$$

Page 270.

On basis/base $p_6 = 19$:

$$M_{16} = (0, 0, 0, 0, 0, 1, 0, 20) \quad k_{16} = 8$$
$$M_{26} = (0, 0, 0, 0, 0, 2, 0, 9) \quad k_{26} = 16$$
$$M_{36} = (0, 0, 0, 0, 0, 3, 0, 28) \quad k_{36} = 5$$
$$M_{46} = (0, 0, 0, 0, 0, 4, 0, 17) \quad k_{46} = 13$$
$$M_{56} = (0, 0, 0, 0, 0, 5, 0, 5) \quad k_{56} = 2$$
$$M_{66} = (0, 0, 0, 0, 0, 6, 0, 25) \quad k_{66} = 10$$
$$M_{76} = (0, 0, 0, 0, 0, 7, 0, 14) \quad k_{76} = 18$$
$$M_{86} = (0, 0, 0, 0, 0, 8, 0, 2) \quad k_{86} = 7$$
$$M_{96} = (0, 0, 0, 0, 0, 9, 0, 22) \quad k_{96} = 15$$
$$M_{10,6} = (0, 0, 0, 0, 0, 10, 0, 10) \quad k_{10,6} = 4$$
$$M_{11,6} = (0, 0, 0, 0, 0, 11, 0, 30) \quad k_{11,6} = 12$$
$$M_{12,6} = (0, 0, 0, 0, 0, 12, 0, 18) \quad k_{12,6} = 1$$
$$M_{13,6} = (0, 0, 0, 0, 0, 13, 0, 7) \quad k_{13,6} = 9$$
$$M_{14,6} = (0, 0, 0, 0, 0, 14, 0, 27) \quad k_{14,6} = 17$$
$$M_{15,6} = (0, 0, 0, 0, 0, 15, 0, 15) \quad k_{15,6} = 6$$
$$M_{16,6} = (0, 0, 0, 0, 0, 16, 0, 4) \quad k_{16,6} = 14$$
$$M_{17,6} = (0, 0, 0, 0, 0, 17, 0, 23) \quad k_{17,6} = 3$$
$$M_{18,6} = (0, 0, 0, 0, 0, 18, 0, 12) \quad k_{18,6} = 11$$

On basis/base $p_7 = 23$:

$$M_{17} = (0, 0, 0, 0, 0, 0, 1, 11) \qquad k_{17} = 5$$
$$M_{27} = (0, 0, 0, 0, 0, 0, 2, 22) \qquad k_{27} = 10$$
$$M_{37} = (0, 0, 0, 0, 0, 0, 3, 2) \qquad k_{37} = 15$$
$$M_{47} = (0, 0, 0, 0, 0, 0, 4, 13) \qquad k_{47} = 20$$
$$M_{57} = (0, 0, 0, 0, 0, 0, 5, 23) \qquad k_{57} = 2$$
$$M_{67} = (0, 0, 0, 0, 0, 0, 6, 3) \qquad k_{67} = 7$$
$$M_{77} = (0, 0, 0, 0, 0, 0, 7, 14) \qquad k_{77} = 12$$
$$M_{87} = (0, 0, 0, 0, 0, 0, 8, 25) \qquad k_{87} = 17$$
$$M_{97} = (0, 0, 0, 0, 0, 0, 9, 5) \qquad k_{97} = 22$$
$$M_{10,7} = (0, 0, 0, 0, 0, 0, 10, 15) \qquad k_{10,7} = 4$$
$$M_{11,7} = (0, 0, 0, 0, 0, 0, 11, 26) \qquad k_{11,7} = 9$$

$$M_{12,7} = (0, 0, 0, 0, 0, 0, 12, 6) \qquad k_{12,7} = 14$$
$$M_{13,7} = (0, 0, 0, 0, 0, 0, 13, 17) \qquad k_{13,7} = 19$$
$$M_{14,7} = (0, 0, 0, 0, 0, 0, 14, 27) \qquad k_{14,7} = 1$$
$$M_{15,7} = (0, 0, 0, 0, 0, 0, 15, 7) \qquad k_{15,7} = 6$$
$$M_{16,7} = (0, 0, 0, 0, 0, 0, 16, 18) \qquad k_{16,7} = 11$$
$$M_{17,7} = (0, 0, 0, 0, 0, 0, 17, 29) \qquad k_{17,7} = 16$$
$$M_{18,7} = (0, 0, 0, 0, 0, 0, 18, 9) \qquad k_{18,7} = 21$$
$$M_{19,7} = (0, 0, 0, 0, 0, 0, 19, 19) \qquad k_{19,7} = 3$$
$$M_{20,7} = (0, 0, 0, 0, 0, 0, 20, 30) \qquad k_{20,7} = 8$$
$$M_{21,7} = (0, 0, 0, 0, 0, 0, 21, 10) \qquad k_{21,7} = 13$$
$$M_{22,7} = (0, 0, 0, 0, 0, 0, 22, 21) \qquad k_{22,7} = 18$$

Page 271.

The parameters of the abbreviated/reduced system of the bases/bases:

$$p_1 = 5, \quad p_2 = 7, \quad p_3 = 11, \quad p_4 = 13, \quad p_5 = 17, \quad p_6 = 19, \quad p_7 = 23,$$

were given during the illustration of method the expansions of range.

Example. To find the minimum trace of the number

$$A = (1, 5, 10, 1, 2, 8, 1, \alpha_{n+1}).$$

We compute the trace

$$S_A = (7 + 23 + 3 + 5 + 10 + 2 + 11) \,(\mathrm{mod}\ 31) = 30.$$

In the abbreviated/reduced system we compute the trace of number A'

$$S'_A = (1 + 10 + 13 + 22 + 19 + 3) \,(\mathrm{mod}\ 23) = 22$$

and its true rank $r_{\mathrm{ист}} = 1 + 5 + 11 + 5 + 6 + 4 = 32 - 10 = 22$. We compute the calculated rank

$$\sum_{i=1}^{n} r_i = 2 + 8 + 1 + 3 = 14$$

and value

$$\left[\frac{22-1}{\rho_n} m_n\right] = 4.$$

Then the value of the minimum trace of a number is determined on (5.72)

$$\alpha_{n+1} = 30 - 22 + 14 + 4 + \Delta_1 = 26 + \Delta_1.$$

Here occurs the inequality

$$(S'_A - \alpha_n)\, m_n \,(\mathrm{mod}\ \rho_n)\, \frac{\nu}{\rho_n} = 13\,\frac{\nu}{\rho_n} > (n-1)\,\frac{\nu}{\rho_n}\,,$$

whence $\Delta_1 = 1$ and $\alpha_{n+1} = S^*_A = 27$. Actually/really, the number

$$A = (1, 5, 10, 1, 2, 8, 1, 27) = 2^{0000}111$$

is correct.

Example. To find the minimum trace of the number

$$A = (0, 3, 10, 12, 11, 14, 5, \alpha_{n+1}).$$

Page 272.

Let us compute the trace

$$S_A = (14 + 3 + 27 + 4 + 27 + 23) \,(\mathrm{mod}\ 31) = 5$$

and trace S'_A of number A'

$$S'_A = (6 + 13 + 15 + 3 + 19) \, (\text{mod } 23) = 10,$$

true rank of which

$$r_{\text{ист}} = 3 + 11 + 6 + 11 + 10 - 2 \cdot 5 = 31,$$

and the calculated rank

$$\sum_{i=1}^{n} r_i = 1 + 8 + 2 + 10 + 5 + 1 = 27.$$

We find

$$\left[\frac{S'_A - \alpha_n}{p_n} \, m_n \right] = 1.$$

On (5.72) we determine the value of the minimum trace of number A

$$\alpha_{n+1} = 5 - 31 + 27 + 1 + \Delta_1 = 2 + \Delta_1.$$

Here

$$(S'_A - \alpha_n) \, m_n \, (\text{mod } p_n) \, \frac{\nu}{p_n} = 2 \, \frac{\nu}{p_n},$$

i.e. value of Λ_1 can have one of two values: 0 or 1, whence the minimum trace of a number can it can have one of two values $\alpha_{n+1}=2$ or $\alpha_{n+1}=3$. i.e. it occurs the critical case.

§5.6. Critical cases.

Both during the use of a method of expanding the range and during the use of a method of reflection onto the end of the range in the standardized/normalized system of bases/bases take the place the indefinite situations when we use with the number

$$A = (\alpha_1, \, \alpha_2, \, \ldots, \, \alpha_n, \, \alpha_{n+1}),$$

about which accurately unknown, it lies/rests at first interval

$[0, \mathscr{P})$ or the secondly $[\mathscr{P}, 2\mathscr{P})$.

Let $\Psi(A)$ - parity of number A, defined as
$$\Psi(A) = \begin{cases} 1, & \text{если число } A \text{ нечетное}, \\ 0, & \text{если число } A \text{ четное}. \end{cases}$$

Key: (1). if a number. (2). odd. (3). even.

Let us consider number $A_\beta = (\alpha_1, \alpha_2, \ldots, \alpha_{n+1}, \beta_{n+1})$, where
$$\beta_{n+1} = \alpha_{n+1} - 1 \,(\mathrm{mod}\, p_{n+1}).$$

Number A_β can be located either in first interval $[0, \mathscr{P})$, if number A was located in the second interval or in latter/last interval $[(p_{n+1} - 1)\mathscr{P}, p_{n+1}\mathscr{P})$, if number A was located in the first interval.

Page 273.

We form by formal division into two number
$$\frac{A_\beta}{2} = \left(\gamma_1, \gamma_2, \ldots, \gamma_n, \frac{\beta_{n-1}}{2} (\mathrm{mod}\, p_{n+1}) \right),$$
where
$$\gamma_i = \frac{\alpha_i}{2} \,(\mathrm{mod}\, p_i),$$
$$i = 1, 2, \ldots, n,$$

and let
$$\Gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n, \gamma_{n+1})$$

- number whose digit γ_{n+1} is obtained by one of the described above methods of determining the minimum trace of a number, moreover is

allowed/assumed critical situation, i.e., it can be found in one of
the first two intervals of numerical range. Then are possible the
following cases.

Case 1. Number A_β even and correct, i.e., is located in interval
$(0, \mathcal{P})$. Quotient from the formal division of number A_β into two will be
the number, also correct in view of parity A_β. A number G can
regarding be found only in one of the first two intervals of
numerical range. Then a difference in the numbers G and $\frac{A_\beta}{2}$ will be

$$
\begin{aligned}
\Gamma - \frac{A_\beta}{2} &= (\gamma_1, \gamma_2, \ldots, \gamma_n, \gamma_{n+1}) - \\
&- \left(\gamma_1, \gamma_2, \ldots, \gamma_n, \frac{\beta_{n-1}}{2} (\bmod p_{n-1})\right) = \\
&= \left(0, 0, \ldots, 0, \left(\gamma_n - \frac{\beta_{n-1}}{2}\right) (\bmod p_{n-1})\right).
\end{aligned}
$$

i.e. if G - correct number, then
$$
\left(\gamma_{n-1} - \frac{\beta_{n-1}}{2}\right) (\bmod p_{n-1}) = 0.
$$

if G - number of the second interval of numerical range, then
$$
\left(\gamma_{n+1} - \frac{\mu_{n-1}}{2}\right) (\bmod p_{n+1}) = \ldots
$$
In general
$$
\left(\gamma_{n+1} - \frac{\beta_{n-1}}{2}\right) (\bmod p_{n+1}) = 1.
$$

Page 274.

Case of 2. Number A_β odd $\psi(A_\beta) = 1$ and correct. Formal quotient
$\frac{A_\beta}{2}$ will be determined whereas

$$
\frac{A_\beta}{2} = \frac{A_\beta + \psi(A_\beta) P}{2} = \frac{p_{n+1} - 1}{2} \psi(A_\beta) \mathcal{P} + \frac{A_\beta + \psi(A_\beta) \mathcal{P}}{2}.
$$

Since

$$\frac{A_\beta + \psi(A_\beta)\,\mathcal{P}}{2} < \mathcal{P},$$

that it is possible to claim that number $\frac{A_\beta}{2}$ is arranged/located in the interval

$$\left[\frac{p_{n+1}-1}{2}\,\mathcal{P},\ \frac{p_{n+1}+1}{2}\,\mathcal{P}\right).$$

Hence the number

$$\Gamma' = (\gamma_1,\ \gamma_2,\ \ldots,\ \gamma_n,\ \beta'_{n+1}),$$

where

$$\beta'_{n+1} = \left(\frac{\beta_{n+1}}{2} - \psi(A_\beta)\frac{p_{n+1}-1}{2}\right)(\bmod\ p_{n+1})$$

it is correct, i.e., occurs the same situation, as in the first case. Then

$$\left(\gamma_{n+1} - \frac{\beta_{n+1}}{2} + \psi(A_\beta)\frac{p_{n+1}-1}{2}\right)(\bmod\ p_{n+1}) < 1.$$

Case of 3. Number A_β is even number, arranged/located in the latter/last interval. Then formal quotient falls into the interval

$$\left[\frac{p_{n+1}-1}{2}\,\mathcal{P},\ \frac{p_{n+1}+1}{2}\,\mathcal{P}\right).$$

Since number A_β can be represented as

$$A_\beta = (p_{n+1}-1)\,\mathcal{P} + \Delta A_\beta,$$

where $\Delta A_\beta < \mathcal{P}$, that

$$\frac{A_\beta}{2} = \frac{p_{n+1}-1}{2}\,\mathcal{P} + \frac{\Delta A_\beta}{2},$$

whence

$$\left(\gamma_{n+1} - \frac{\beta_{n+1}}{2}\right)(\bmod\ p_{n+1}) > \frac{p_{n+1}-1}{2}.$$

Page 275.

Case of 4. Number A_β is an odd and incorrect number of interval

$((p_{n+1}-1)\mathscr{P},\ p_{n+1}\mathscr{P})$, and quotient from the formal division of number A_β into two will be

$$\frac{A_\beta}{2}=\frac{A_\beta+p_{n+1}\mathscr{P}}{2}=\frac{(p_{n+1}-1)\mathscr{P}+\Delta A_\beta+p_{n+1}\mathscr{P}}{2},$$

where $\Delta A_\beta<\mathscr{P}$ or

$$\frac{A_\beta}{2}=p_{n+1}\mathscr{P}-\frac{\mathscr{P}-\Delta A_\beta}{2}.$$

Since $\mathscr{P}-\Delta A_\beta<\mathscr{P}$, that it is possible to claim that number $\frac{A_\beta}{2}$ is arranged/located in the latter/last interval, i.e.,

$$(p_{n+1}-1)\mathscr{P}<\frac{A_\beta}{2}<p_{n+1}\mathscr{P}.$$

Then

$$\left(\gamma_{n+1}-\frac{\beta_{n+1}}{2}+\psi(A_\beta)\frac{p_{n+1}-1}{2}\right)(\mathrm{mod}\ p_{n+1})>\frac{p_{n+1}-1}{2}.$$

Summarizing, it is possible to formulate the criterion of the correctness of number A_β as follows: number A_β correct, if occurs the condition

$$\left(\gamma_{n+1}-\frac{\beta_{n+1}}{2}+\psi(A_\beta)\frac{p_{n+1}-1}{2}\right)(\mathrm{mod}\ p_{n+1})\leqslant 1.\quad(5.74)$$

Thus, in the critical cases we can use criterion (5.74) for solving the alternative, what number is the unknown correct number A or A_β.

Let us consider now some theorems, which connect characteristics (of type of rank, trace, character, etc.) of numbers G and A.

Theorem 5.18. If in the system of bases/bases $p_1,\ p_2,\ \dots,\ p_n$, with weights of orthogonal bases of $m_1,\ m_2,\ \dots,\ m_n$, is preset number $A'=(\alpha_1,\ \alpha_2,\ \dots,\ \alpha_{n-1},\ \alpha_n)$, true rank of which r'_A, and parity $\psi(A')$, then the

true rank of number $\Gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n)$, of the obtained by formal division number A' into two, will be defined as

$$r_\Gamma = \frac{1}{2}\left(r'_A + \sum_{i=1}^{n} m_i \psi(\alpha_i) - \psi(A')\right). \qquad (5.75)$$

where $\psi(\alpha_i)$ there is a function of the parity of values α_i.

Proof. Let us first demonstrate theorem on the assumption that number A' even i.e. $\psi(A') = 0$.

Page 276.

In this case upon the doubling formal particular G the transition through the range cannot occur, i.e.,

$$\Gamma + \Gamma = 2\Gamma = A'.$$

whence according to the theorem about the rank of sum follows

$$r'_A = 2r_\Gamma - \sum_{i=1}^{n} m_i \psi(\alpha_i).$$

By this is proved validity (5.75) for the the even A'. Let it be now initial number A' odd, i.e., $\psi(A') = 1$. Then upon the doubling of formal quotient occurs one transition through the range i.e.

$$\Gamma + \Gamma = 2\Gamma = A' + \mathcal{P}\psi(A').$$

whence

$$r'_A = 2r_\Gamma - \sum_{i=1}^{n} m_i \psi(\alpha_i) - \psi(A').$$

Consequently (5.75) is correct for the the odd A'.

Theorem 5.19. If is preset the system of bases/bases $p_1, p_2, \ldots, p_n$

with weights of orthogonal bases of $m_1, m_2, \ldots, m_n$ and the expanded system of bases/bases $p_1, p_2, \ldots, p_n, p_{n+1}$ with weights of orthogonal bases of $\tilde{m}_1, \tilde{m}_2, \ldots, \tilde{m}_n, \tilde{m}_{n+1}$ is known value $\sigma_{A'}$ - the generalized sum of the digits of the number

$$A' = (\alpha_1, \alpha_2, \ldots, \alpha_n),$$

the value σ_Γ of the generalized sum of the digits of the number

$$\Gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n),$$

the obtained by formal division number A' into two, will be determined from the condition

$$\sigma_\Gamma = \frac{1}{2} \left(\sigma_{A'} - p_{n+1} \sum_{i=1}^{n} \tilde{m}_i \psi(\alpha_i) - \sum_{i=1}^{n} m_i \psi(\alpha_i) \right). \quad (5.76)$$

Proof. Since according to the condition a number G is obtained by the formal division of number A' into two, then for all $i = 1, 2, \ldots n$ takes the place

$$\gamma_i = \frac{\alpha_i - p_i \psi(\alpha_i)}{2}.$$

Page 277.

Regarding the generalized sum of the digits

$$\sigma_\Gamma = \sum_{i=1}^{n} \left(\frac{\tilde{m}_i p_{n+1} - m_i}{p_i} \right) \left(\frac{\alpha_i - p_i \psi(\alpha_i)}{2} \right) =$$

$$= \frac{1}{2} \left(\sigma_{A'} - \sum_{i=1}^{n} (\tilde{m}_i p_{n+1} - m_i) \psi(\alpha_i) \right),$$

which coincides with assertion (5.76) of theorem.

Corollary 1. If the values of the generalized sums of the digits of numbers A' and G are presented in the form

$$\sigma_{A'} = \varkappa_1 p_{n+1} - q_{A'},$$

$$\sigma_{\Gamma} = \varkappa_2 p_{n+1} - q_{\Gamma}.$$

where $\varkappa_1, \varkappa_2, q_{A'}, q_{\Gamma}$ - whole non-negative numbers, moreover

$$q_{A'} < p_{n+1},$$

$$q_{\Gamma} < p_{n+1}.$$

then occurs the equality

$$q_{\Gamma} = \frac{1}{2}\left(q_{A'} - \sum_{i=1}^{n} m_i \psi(\alpha_i)\right) \pmod{p_{n+1}}. \qquad (5.77)$$

Actually/really, condition (5.76) can be represented in the form

$$2\varkappa_2 p_{n+1} - 2q_{\Gamma} = \varkappa_1 p_{n+1} - q_{A'} + p_{n+1} \sum_{i=1}^{n} \tilde{m}_i \psi(\alpha_i) - $$

$$ - \sum_{i=1}^{n} m_i \psi(\alpha_i),$$

or

$$2q_{\Gamma} = p_{n+1}\left(2\varkappa_2 - \varkappa_1 - \sum_{i=1}^{n} \tilde{m}_i \psi(\alpha_i)\right) - q_{A'} - \sum_{i=1}^{n} m_i \psi(\alpha_i).$$

Page 278.

After introducing the designations:

$$\varkappa_3 = 2\varkappa_2 - \varkappa_1 - \sum_{i=1} \tilde{m}_i \psi(\alpha_i),$$

$$q = q_{A'} + \sum_{i=1}^{n} m_i \psi(\alpha_i).$$

we will obtain

$$2q_{\Gamma} = p_{n+1}\varkappa_3 + q.$$

Since p_{n+1} - odd basis/base, and on the left side of the expression will cost even number, then it is possible to claim that values $\varkappa_3$ and q have identical parity. Then, if $\varkappa_3$ and q - even values, takes the place

$$q_\Gamma = p_{n-1}\frac{x_3}{2} + \frac{q}{2}$$

or

$$q_\Gamma \equiv \frac{1}{2}q \pmod{p_{n+1}}.$$

If x_3 and q - odd values, then has the place

$$q_\Gamma = p_{n+1}\frac{x_3-1}{2} + \frac{p_{n+1}+q}{2}$$

or

$$q_\Gamma \equiv \frac{1}{2}q \pmod{p_{n+1}}.$$

Hence

$$q_\Gamma \equiv \frac{1}{2}\left(q_{A'} + \sum_{i=1}^{n} m_i\psi(\alpha_i)\right) \pmod{p_{n+1}},$$

which coincides with (5.77).

Theorem 5.20. If in the expanded system of the bases/bases

$$p_1, p_2, \ldots, p_n, p_{n+1}$$

is obtained by the expansion of range the number

$$A' = (\alpha_1, \alpha_2, \ldots, \alpha_n, x_{n+1})$$

of parity $\psi(A')$, then for the number

$$\Gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n, \gamma_{n+1}),$$

where

$$\gamma_i = \frac{\alpha_i}{2} \pmod{p_i},$$

on the basis of p_{n+1}, $i = 1, 2, \ldots, n,$

the value of digit γ_{n+1} with which a number G is correct, it is determined from the condition

$$\widetilde{m}_{n+1}\gamma_{n+1} = \frac{\widetilde{m}_{n+1}\alpha_{n+1} + \psi(A')}{2} \pmod{p_{n+1}}. \qquad (5.78)$$

Page 279.

Proof. The value of digit γ_{n+1} of a number G in the expanded representation is defined as

$$\widetilde{m}_{n+1}\gamma_{n+1} = \frac{1}{2}(q_{A'} - r_{A'} + \psi(A'))\ (\text{mod}\ p_{n+1}),$$

whence and follows confirmation (5.78) of the theorem.

Corollary. In the standardized/normalized system of bases/bases condition (5.78) accepts the form

$$\gamma_{n+1} = \frac{\alpha_{n+1} + \psi(A')}{2}\ (\text{mod}\ p_{n+1}). \qquad (5.79)$$

The criterion of the correctness of number A_B, taking into account (5.79) and

$$\beta_{n+1} = \alpha_{n+1} - 1\ (\text{mod}\ p_{n+1}),$$

an example the form

$$\left(\frac{1 + \psi(A)}{2} + \psi(A_B)\frac{p_{n+1} - 1}{2}\right)(\text{mod}\ p_{n+1}) \leqslant 1 \qquad (5.80)$$

can be formulated as follows: if the parities of numbers A also A_B coincide, then correct is a number A. If the parity of numbers A also A_B different, then correct is number A_B.

Let us consider how can be determined the parity of a number A.

For forming the number of form $M_A = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A)$ stored/added up the minimum numbers, which are the constants of system. After designating through $\psi(k_{ij})$ the function of the parity of the

multiplicity of corresponding component/term/addend, it is possible
to claim that the parity of number M_A will be defined as

$$\psi(M_A) = \sum_{i=1}^{n-1} \psi(k_{ij}) \pmod 2.$$

Further was conducted the expansion of number M_A, but in this
case a number did not vary in the value and, that means did not vary
its parity.

For forming the number A to number M_A they adjoined constant
$\tilde{M}_{\beta n}$ of parity $\psi(\tilde{M}_{\beta n})$. Since in this case the transition through the
range is impossible, then the parity of a number A will be defined as

$$\psi(A) = \left(\sum_{i=1}^{n-1} \psi(k_{ij}) + \psi(\tilde{M}_{\beta n}) \right) \pmod 2. \qquad (5.81)$$

Page 280.

For determining the parity $\psi(A_\beta)$ let us consider value

$$N' = \left(\frac{\beta_{n+1}}{2} - \gamma_{n+1} \right) \pmod{p_{n+1}},$$

which determines a number of intervals, which divide the numbers

$$\Gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n, \gamma_{n+1})$$

and

$$\Gamma' = \frac{A_\beta}{2} = \left(\gamma_1, \gamma_2, \ldots, \gamma_n, \frac{\beta_{n+1}}{2} \pmod{p_{n+1}} \right).$$

In this case are possible the following cases.

Case 1. If $N' < \frac{p_{n+1}-1}{2}$, then upon the doubling of a number β' does
not have a point of emergence for the range, but obtained as a result
of doubling number A ever, i.e., $\psi(A_\beta) = 0$.

Case of 2. If $N' > \frac{p_{n+1}-1}{2}$, then upon the doubling of a number it takes place for the range, and therefore, obtained as a result of doubling number A_β odd, i.e., $\psi(A_\beta) = 1$.

Case of 3. If $N' = \frac{p_{n+1}-1}{2}$, then in accordance with the theorem about the parity of a number we have

$$\psi(A_\beta) = (\psi(\beta_{n+1}) + \psi(S_{A_\beta}) + \psi(\lambda))(\text{mod } 2), \quad (5.82)$$

where λ - number of incorrect digits in number A_β.

Now can be formulated the third version of the criterion of the correctness of the number: if $N' < \frac{p_{n+1}-1}{2}$, then correct is number A_β. If $N' \geqslant \frac{p_{n+1}+1}{2}$, then correct is number A. If $N' = \frac{p_{n+1}-1}{2}$, then when $\psi(A_\beta) = 1$ correct will be number A, and when $\psi(A_\beta) = 0$ correct will be number A_β.

Let be preset the basic system of the bases/bases:

$$p_1 = 5; \quad p_2 = 7; \quad p_3 = 11; \quad p_4 = 13; \quad p_5 = 17; \quad p_6 = 19; \quad p_7 = 23,$$

with range $\mathscr{P} = 37182145$. parameters of which are given on page 249. As the expanded system let us take

$$p_1 = 5; \quad p_2 = 7; \quad p_3 = 11; \quad p_4 = 13; \quad p_5 = 17; \quad p_6 = 19; \quad p_7 = 23; \quad p_8 = 31.$$

Range of this system $\mathscr{P} = 1152646495$. The parameters of this system are given on page 268.

For the basic and expanded systems of value λ accept the following values:

$$\lambda_1 = 21, \quad \lambda_2 = 26, \quad \lambda_3 = 2, \quad \lambda_4 = 26, \quad \lambda_5 = 10, \quad \lambda_6 = 11, \quad \lambda_7 = 20.$$

Example. To determine the number of the interval in which is located the number

$$A = (0, 1, 4, 2, 16, 13, 21, 9).$$

Page 281.

Let us find first values α_{n+1} with which the number

$$A = (0, 1, 4, 2, 16, 13, 21, \alpha_{n+1})$$

it is correct, i.e., it is arranged/located in the first interval. let us find the trace of this number S_A in the basic system

$$S_A = (2 + 8 + 21 - 9 - 21) \,(\text{mod } 23) = 15.$$

In this case occurred two transitions through basis/base $p_7 = 23$, i.e., $\pi_A = 2$. Thus, in the basic system it is possible to form the number

$$M_A = (0, 1, 4, 2, 16, 13, 15).$$

rank of which is equal to

$$r_{M_A} = 1 - 5 - 5 - 17 - 10 - 2.5 \quad 28.$$

Let us compute generalized sum of the digits of a number A

$$\sigma_A = 26 + 8 + 52 - 160 + 143 - 300 = 23 \cdot 31 - 24.$$

Consequently

$$q = 24.$$

Then

$$\alpha_{n+1} = (24 - 28) \,(\text{mod } 31) = 27.$$

We form the expanded representation of number M_A

$$M_A = (0, 1, 4, 2, 16, 13, 15, 27).$$

In order on foundation for p_7 obtaining digit $\alpha_7 = 21$, it is necessary to the obtained number to adjoin the number

$$\tilde{M}_7 = (0, 0, 0, 0, 0, 0, 6, 3)$$

of multiplicity $k_7 = 7$.

Since has place $k_7 < p_n - n - 1$, then the obtained sum

$$A_1 = M_A + \tilde{M}_7 = (0, 1, 4, 2, 16, 13, 21, 30)$$

is the unknown correct number.

Actually/really

$$A_1 = (0, 1, 4, 2, 16, 13, 21, 30) = 15 \cdot 10^6,$$

i.e. it lies/rests at the first interval of the expanded system. An initial number A is located in interval $[10\mathcal{F}, 11\mathcal{F})$.

Example. To determine the digit α_8, with which the number

$$A_1 = (3, 3, 3, 3, 3, 3, 3)$$

will be correct in the expanded range. Let us compute the trace of number A_1 in the basic system

$$S_A = (12 - 6 - 21 - 20 - 1 - 8) \pmod{23} = 22.$$

In this case occurred two transitions through basis/base p_7, i.e., $\tau_1 = 2$. We form number M_A:

$$M_A = (3, 3, 6, 1, 3, 3, 22).$$

rank of which

$$r_{M_A} = 5 - 3 - 7 - 5 - 3 - 5 - 10 = 16.$$

Page 282.

Let us determine the value of the generalized sum of the digits

$$\sigma_A = 72 + 78 + 6 + 78 + 30 + 33 + 440 = 24 \cdot 31 - 7,$$

whence.

$$\alpha_{n+1} = (7 - 16) \, (\text{mod } 31) = 22.$$

Thus obtained the expanded representation of a number M_A

$$M_A = (3, 3, 3, 3, 3, 3, 22, 22).$$

As constant $\widetilde{M}_7$, it must be selected

$$\widetilde{M}_7 = (0, 0, 0, 0, 0, 0, 4, 13)$$

multiplicity $k_7 = 20$. Here occurs the critical situation

$$k_7 > p_7 - n + 1.$$

i.e. that obtained of number $A_2 = M_A + \widetilde{M}_7 = (3, 3, 3, 3, 3, 3, 3, 4)$ lies/rests either at the first or in the second interval. As can easily be seen in this case.

Then.

$$\psi(A_2) = \sum_{i=1}^{n-1} \psi(k_{ij}) \, (\text{mod } 2) = 0.$$

$$\gamma_{n+1} = 2.$$

Let us find

$$\frac{\beta_{n+1}}{2} = \frac{3}{2} \, (\text{mod } 31) = 17,$$

whence

$$N' = 15,$$

i.e. it occurs the case $N' = \dfrac{p_{n+1}-1}{2}$.

After using the theorem about the parity of a number, we will obtain.

$$\psi(A_\beta) = (\psi(3) + \psi(S_{A_\beta}) + \psi(\lambda)) \pmod 2.$$

Here $\psi(3) = 1$. Let us find the values

$$\psi(S_{A_\beta}) = (1 + 0 + 1 + 1 + 0 + 0 + 0) \pmod 2 = 1,$$
$$\psi(\lambda) = (0 + 1 + 1 + 1 + 1 + 0 + 1) \pmod 2 = 0.$$

We obtain $\psi(A_\beta) = 0$. According to the third version of the criterion of correctness we establish that a correct number is a number.

$$A = (3, 3, 3, 3, 3, 3, 3, 3).$$

Is actual/real, $A = 3 < P$.

Page 283.

§5.7. On nonmodular operations.

The nonmodular operations include the operations, which carry positional character, i.e., using with the value of entire number as a whole, but not with its representations, undertaken according to the independent foundations isolated/insulated. From this point of view nonmodular operations relate to a number of positional

operations, i.e., most difficult operations in the system of residual
classes.

Further difficulty creates the circumstance that the arithmetic
unit, which works in the residual classes, is expedient to realize in
the form of the independent blocks, which work on the independent
foundations and those not virtually connected. Therefore the
algorithms of the execution of nonmodular operations must be
constructed on the basis of their realization in the nonpositional
arithmetic unit.

The examined in present chapter methods of numbering of the
interval in which is arranged/located a number or, which is the same
thing, the methods of determining the minimum trace of a number, make
it possible to obtain the evaluation of the number being investigated
in its value with an accuracy to the value of interval, which, in
turn, makes it possible to find the efficient algorithms of the
execution of the majority of nonmodular operations. Widely can be
used for the same purpose the traced in Chapter 3 criterion of
overflow for the addition of numbers.

Let to us be preset the regulated system of bases/bases
$p_1, p_2, \ldots, p_n$, whose numerical range $\mathcal{P}$ is decomposed on P_n intervals by
value

$$\left[j \frac{\mathscr{P}}{p_n}, (j+1) \frac{\mathscr{P}}{p_n} \right).$$

As second computer zero let us select the point of numerical range $\frac{p_n+1}{2} \frac{\mathscr{P}}{p_n}$. The numbers, arranged/located in sub-ranges $\left[0, \frac{p_n+1}{2} \frac{\mathscr{P}}{p_n} \right)$ and $\left[\frac{p_n-1}{2} \frac{\mathscr{P}}{p_n}, \mathscr{P} \right)$, we will consider numbers of different signs. Let us agree for the certainties of a number, which lie at sub-range $\left[0, \frac{p_n+1}{2} \frac{\mathscr{P}}{p_n} \right)$ or at the intervals with numbers $0, 1, 2, \ldots, \frac{p_n-1}{2}$, to consider it negative, and the numbers, which lie at sub-range $\left[\frac{p_n-1}{2} \frac{\mathscr{P}}{p_n}, \mathscr{P} \right)$ or at the intervals with numbers $\frac{p_n-1}{2}, \frac{p_n+3}{2}, \ldots, p_n-1,$ - positive.

Page 284.

But then a question about the determination of the sign of a number is reduced to numbering of the interval in which is arranged/located a number. Any of the examined in present chapter methods of determination of the number of the interval in which is arranged/located a number, automatically determines its sign, and during the use of a method of the evaluation of intervals the sign of a number can be determined already in the stage of determination of the type of the criticality of a number, since first type critical number is always located in the intervals to the left of $\frac{p_n+1}{2}$ and, therefore, this number negative. On the contrary, second type critical number is located in the ranges, close to $\mathscr{P}$, to the right of

$\frac{p_n - 1}{2}$, this number positive.

Let us consider the now arithmetic comparison of two numbers. Let be preset two numbers A and B is required to determine, which of the numbers is more. Let us determine by one of the described above methods of the number of the intervals in which are arranged/located these numbers.

Let number A be is arranged/located in interval of j_1, and number B - in interval of j_2. Then in the case of $j_1 \neq j_2$ the operation of arithmetic comparison can be realized simply by the comparison of the numbers of intervals, namely, if $j_1 > j_2$, then A>B, and if $j_1 < j_2$, then A<B. Exception/elimination comprises case $j_1 = j_2$. Here for determining the larger number it is necessary to determine number j_3 of the interval in which is arranged/located difference A-B. If $0 \leqslant j_3 < \frac{p_n - 1}{2}$, then difference is negative, and hence A<B. If $\frac{p_n + 1}{2} \leqslant j_3 < p_n$, then difference positive and A>B.

And finally if A-B=0, then numbers A and B are identical with respect to value and sign.

Nonmodular operations include also the operation of the translation of numbers of one numeration system into another, most frequently of decimal or binary into the system of residual classes

and vice versa. The translation/conversion from any positional system
into the system of residual classes does not represent work.

Let be is preset the representation of number A in the
positional numeration system in the form

$$A = a_n p^n + a_{n-1} p^{n-1} + \ldots + a_2 p^2 + a_1 p + a_0.$$

where p_n - basis of system, and value a_i satisfies inequality
$0 < a_i < p$, $i = 0, 1, 2, \ldots, n$.

Page 285.

Having a set of constants, represented in the residual classes and
corresponding to numbers $0, 1, 2, \ldots, p^n$, it is possible, by computing
consecutively/serially values $a_i p^i$ and storing/adding up them in the
arithmetic unit, which works in the system of residual classes, to
obtain the nonpositional representation of a number.

Just as simply is produced the translation/conversion from the
system of residual classes into the positional numeration system.

Let in the system of bases/bases $p_1, p_2, \ldots, p_n$ be is preset number
$A = (a_1, a_2, \ldots, a_n)$, which is the numerator of the proper fraction whose
denominator j. Is required number A to present in the form of correct

binary fraction, namely:

$$A = 2^{-1}\varepsilon_1 + 2^{-2}\varepsilon_2 + \ldots + 2^{-s}\varepsilon_s.$$

The conversion indicated can be carried out by the following sequence of operations.

First step/pitch. We compute sum of $A + A = 2A$ and simultaneously compute the criterion of overflow Ω_{2A}, whose value is high-order digit of the binary notation of a number, i.e.

$$\Omega_{2A} = \varepsilon_1.$$

Second step/pitch. We compute sum $2A + 2A = 4A$. The value of the criterion of overflow Ω_{4A} is the digit of the second after comma bit.

$$\Omega_{4A} = \varepsilon_2.$$

Repeating this process of s of times, we will obtain the binary notation of number A in the form

$$A = 2^{-1}\varepsilon_1 + 2^{-2}\varepsilon_2 + \ldots + 2^{-s}\varepsilon_s.$$

where

$$\varepsilon_i = \Omega_{2^i A}, \quad i = 1, 2, \ldots, s.$$

In this case can be easily written the routine of translation/conversion, based on this method. It in essence will consist of the the consecutive of an addition-calculation of the criteria of overflow and shifts/shears of the obtained digits of the binary equivalent of this fraction.

Let us consider the now interrogatory method of obtaining the

binary equivalent number.

Let number $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ be the numerator of the proper fraction whose denominator lies/rests within the limits

$$2^t < \mathscr{P} < 2^{t-1}.$$

Page 286.

It is required to find the binary equivalent of number A. Let us present equivalents in the residual classes of the binary values 2^j

$$2^j = (\mu_1^{(j)}, \mu_2^{(j)}, \ldots, \mu_n^{(j)}),$$
$$j = 1, 2, \ldots, t.$$

Let us compute difference in the residual classes.

$$A - 2^t = \Delta_t.$$

Let us determine sign sign Δ_t value Δ_t. The inverse value $\overline{\text{sign } \Delta_t}$ will be binary high-order digit of the binary equivalent of a number

$$\varepsilon_1 = \overline{\text{sign } \Delta_t}.$$

Further, from Δ_t or from the restored/reduced with negative Δ_t number A subtrahend is equivalent in the residual classes of binary value 2^{t-1}. In this case we obtain value Δ_{t-1}. The inverse value of sign Δ_{t-1} is the following digit of the binary equivalent of number A

$$\varepsilon_2 = \overline{\text{sign } \Delta_{t-1}}.$$

Analogously are determined the remaining digits of the binary equivalent of an initial number. The procedure indicated can be organized, also, without the restoration/reduction of negative

remainder/residue. For this together with the equivalents in the
residual classes of values 2^j by equivalents in the residual classes
of values 2^j it is necessary to have equivalents of two's to
complements.

    As the modification of this method let us consider the
translation/conversion into the binary-coded decimal system.

    Let $\mathscr{P}$ lies/rests within limits $10' < \mathscr{P} < 10^{s+1}$. Let us take set
$4(s+1)$ the constants, which are equivalents in the residual classes
of the values:

$$c_{0i} = 10^i,$$
$$c_{1i} = 2 \cdot 10^i,$$
$$c_{2i} = 2^2 \cdot 10^i,$$
$$c_{3i} = 2^3 \cdot 10^i,$$
$$i = 0, 1, 2, \ldots, s.$$

Page 287.

    Subtrahend from A value c_{3s}. If difference is positive, then c_{3s}
is determined the senior tetrad of binary equivalent, if difference
is negative, from A is subtracted c_{2s}. If difference during this
subtraction is positive, then the digit of senior tetrad is
determined, otherwise from A is subtracted c_{1s}. Even if in this case
the digit of senior tetrad is not determined, from A is subtracted
c_{0s}. Continuing further this process, we obtain the binary-coded

decimal equivalent of number A.

Let us consider now the algorithm of the rounding of number A:
$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n),$$
to r of significant digits r<n.

In the positional system with basis/base p number A will be represented in the form

$$A = \delta_1 p^{m-1} + \delta_2 p^{m-2} + \ldots + \delta_m = (\delta_1, \delta_2, \ldots, \delta_m).$$

The rounding of number A to r of significant digits on basis/base p consists in the replacement of digits $\delta_m, \delta_{m-1}, \ldots, \delta_{r+1}$ by zero. In other words the rounded-off to r digits number A will take in the positional numeration system the following form:.

$$A_{\text{окр}} = (\delta_1, \delta_2, \ldots, \delta_r, 0, 0, \ldots, 0).$$

From an arithmetic point of view this rounding is subtraction from A of the rounding off number a, where

$$a = (0, 0, \ldots, 0, \delta_{r+1}, \delta_{r+2}, \ldots, \delta_n).$$

When A is integer, the execution of the operation of rounding is finished with the procedure indicated.

But if A is fraction, by kA to this procedure is adjoined even crossing out of zeros, obtained in the end digits of a number.

Arithmetically this crossing out is nothing else but the division of a number on p^{m-r}.

Thus, the realization of the operation of rounding leads to the following procedure:

1) is revealed/detected the rounding off number a:

2) is revealed/detected difference A-a:

3) are divided A-a into p^{m-r}.

It is possible the process of rounding indicated to implement consecutively/serially, namely:

1) to determine the next digit δ_i;

2) to subtract δ_i from A:

3) to divide difference $A - \delta_i$ into p.

Page 288.

Analogously to act with the obtained result consecutively/serially (n-r) of times.

Let us consider now on the basis of the theory of ranks the
process of division into 10 in the absence in the composition of the
bases/bases of the dividers/denominators of number 10, i.e., in the
absence of zero values among the digits of the divider/denominator,
represented in the selected system of bases/bases. Then division can
be produced step-by-step. When dividend is multiple 10, result will
be exact quotient. Let us consider, which is result in the case, the
code dividend is not multiple 10.

Assume it is necessary to divide number A into 10 and let
A=10s+t. Dale it is step-by-step A to 10, we will obtain

$$a = \frac{10s + t - k\mathscr{P}}{10} = s + \frac{t + k\mathscr{P}}{10} \ .$$

Thus $t - k\mathscr{P}$ it shares by 10. If we take for simplicity such
bases/bases that the last figure $\mathscr{P}$ would be equal to 1, then in this
case sum t+k=10 or t=10-k. As far as value is concerned k, then this
the difference in the ranks of a number 10a and actual dividend,
i.e., for obtaining the latter/last decimal digit of actual dividend
should be computed the rank of product 10a. Thus, it is possible to
determine the value of the last figure of the decimal representation
A as follows:

1) we divide step-by-step dividend by 10;

2) we compute the rank of quotient;

3) is computed rank 10a (but thereby we determine the last figure of actual dividend).

Let us illustrate the given method of determining the latter/last decimal digit of dividend.

Let us take numeration system with bases/bases $p_1=3$; $p_2=7$; $p_3=11$. The range of system will be defined as $\mathscr{P} = 3 \cdot 7 \cdot 11 = 231$. By orthogonal bases will be $B_1=154$, $B_2=99$, $B_3=210$, and their weights respectively $m_1=2$, $m_2=3$, $m_3=10$.

Example. To find the latter/last decimal digit of number $A=(2, 0, 8)$ with rank $r_A = 8$. Number 10 in the selected numeration system will be represented $10=(1, 3, 10)$ with rank $r_{10}=11$. Dale it is step-by-step A to 10, we will obtain $a=(2, 0, 3)$. It is easy to compute the rank of number a: $r_a = 4$. The rank of a number 10a will be defined as

$$r_{10a} = 4 \cdot 10 - \left[\frac{20}{3} \right] 2 - \left[\frac{30}{11} \right] 10 = 8.$$

Page 289.

Here the difference of the ranks of number A and number 10a is equal to zero, whence it follows that the latter/last decimal digit of number A is equal to zero, i.e. A is multiple 10, and the obtained result is true quotient. Is actual/real A=(2, 0, 8)=140.

Example. To find the latter/last decimal digit of number A=(2, 5, 8) with rank r_A =10 and to round off it to one decimal digit. Dale A to 10, we will obtain a=(2, 4, 3). Let us compute its rank - r_a =5. We compute the rank r_{10a}

$$r_{10a} = 50 - \left[\frac{20}{3}\right] 2 - \left[\frac{40}{7}\right] 3 - \left[\frac{30}{11}\right] 10 = 3.$$

Hence k=10-3=7, t=10-7=3. The last figure of decimal representation exists 3=(0, 3, 3). After subtracting from A number 3, we obtain the number

$$(2, 5, 8) - (0, 3, 3) = (2, 2, 5).$$

which during the division into 10 gives

$$(2, 2, 5) : (1, 3, 10) = (2, 3, 6) = 17.$$

Thereby is carried out the rounding of number 173 to one digit.

Until now, was examined the rounding of a number in the residual classes to one decimal digit. However, rounding can be conducted immediately, also, on the arbitrary quantity q of digits. For this it

is necessary to divide an initial number not into 10, but into 10^q.

Let us consider an example with the rounding to two decimal digits. In this case for the divider/denominator is accepted a number $10^2 = 100 = (1, 2, 1)$, with rank $r_{100} = 2$.

Example. To find the latter/last two decimal digits of number $A = (2, 3, 8)$ with rank $r_A = 9$ and to round off it to two decimal digits.

Dale is step-by-step number A to 100, we will obtain quotient

$$a = (2, 3, 8) : (1, 2, 1) = (2, 5, 8).$$

As can easily be seen, its rank is equal to $r_a = 10$. Let us compute the rank of value 100a

$$r_{100a} = 100r_a - \left[\frac{200}{3}\right] 2 - \left[\frac{500}{7}\right] 3 - \left[\frac{800}{11}\right] 10 = -65.$$

Then a difference in the ranks of actual and rounded-off dividends will be

$$k = r_A - r_{100a} = 74.$$

Latter/last 2 digits are computed from those considerations so that $k \cdot 231 + t$ would be finished by two zero. If bases/bases were selected then so that the latter/last 2 digits $\wp$ would be 01, then t would be equal to 100-k. In this case the latter/last 2 digits of product $74 \cdot 231$ are 94 and, therefore, t=100-94=06.

Thus, the latter/last 2 digits A are $06 = (0, 6, 6)$. Subtrahend from A number 06

$$(2, 3, 8) - (0, 6, 6) = (2, 4, 2)$$

we divide result for 100, i.e., (2, 4, 2):(1, 2, 1)=(2, 2, 2). We
will obtain the quotient (2, 2, 2), which is the rounding of number
(2, 3, 8) to 2 decimal digits.

Page 290.

From all that has been previously stated, it follows that the
described procedure of rounding can be carried out to any numerical
length. Since in this case are conducted the operations above the
ranks, then it is expedient to represent ranks in the same system of
residual classes so that all operations would be conducted uniformly.

The nonmodular to operations include the shifts/shears of
mantissa to the left and to the right on q of digits.

In the positional system with basis/base p the shift/shear of
mantissa is to the left produced by the appropriate displacement to
the left of the code of mantissa and by replacement by zero newly
appearing to the right digits. From an arithmetic point of view this
indicates multiplication A on p^q. Knowing the representation of number
p^q in the system of residual classes, it is possible by
multiplication A by this number to obtain the result, equivalent to
shift/shear on q of the digits in the positional representation of
number A. The possibility of multiplication immediately on p^q (i.e.

the knowledge of representation in the system of the

remainders/residues of value p^q for any q) is analogous to the

presence of the register, which shifts the code to any numerical

length.

It is possible to realize multiplication on p^q by the

consecutive multiplications q of times by number p, represented in

the system of residual classes. Here it suffices to only know the

appropriate representation p. This path is analogous to the presence

of register with the shift/shear of the code to one digit.

Example. Bases/bases: $p_1=2$; $p_2=5$; $p_3=7$; $p_4=23$. Let A=13= (1, 3,

6, 13). It is necessary to shift number A to the left by 2 decimal

digits, i.e., $p^2 = 100 = (0, 0, 2, 8)$; $A_{сдв} = A \cdot 100 = (1, 3, 6, 13)(0, 0, 2, 8) = (0, 0, 5, 12)$. Is

actual/real, $A_{сдв} = (0, 0, 5, 12) = 1300$.

Using a number 10=(0, 0, 3, 10) it is possible the same

operation to fulfill consecutively/serially

$$A_{сдв} = (A \cdot 10) \, 10 = ((1, 3, 6, 13)(0, 0, 3, 10))(0, 0, 3, 10) =$$
$$= (0, 0, 4, 15)(0, 0, 3, 10) = (0, 0, 5, 12).$$

The shift/shear of mantissa on q digits is to the right produced

by the displacement/movement of the code of mantissa on q of digits

to the right with the rejection of digits low-order q digits and by

replacement by zero newly appearing to the left q digits.

The arithmetic content of this operation is of the subtraction of the number, formed low-order q digits and division of the obtained difference on 10^q.

In conclusion let us consider the algorithm of the execution of the frequently met operation of dividing the number A into one of the basis p_i of the system of bases/bases.

Page 291.

In the case of dividing the number A into basis/base p_i, when the minimum trace of dividend is unknown, determination by its method of nulling can be combined with the determination of the digit of quotient $\frac{A}{p_i}$ from basis/base p_i

Let in the system of bases/bases $p_1, p_2, \ldots, p_n$ be is preset number $A = (\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n)$, quotient of the division of which into basis/base p_i are $\frac{A}{p_i} = (\gamma_1, \gamma_2, \ldots, \gamma_n)$.

Let $\overline{M}_{\alpha_1} = (\alpha_1, \alpha_2^{(1)}, \ldots, \alpha_{i-1}^{(1)}, 0, \alpha_{i-1}^{(1)}, \ldots, \alpha_n^{(1)})$ small from the numbers, which separate on p_i and those having digit α_1 on basis/base p_1.

MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU
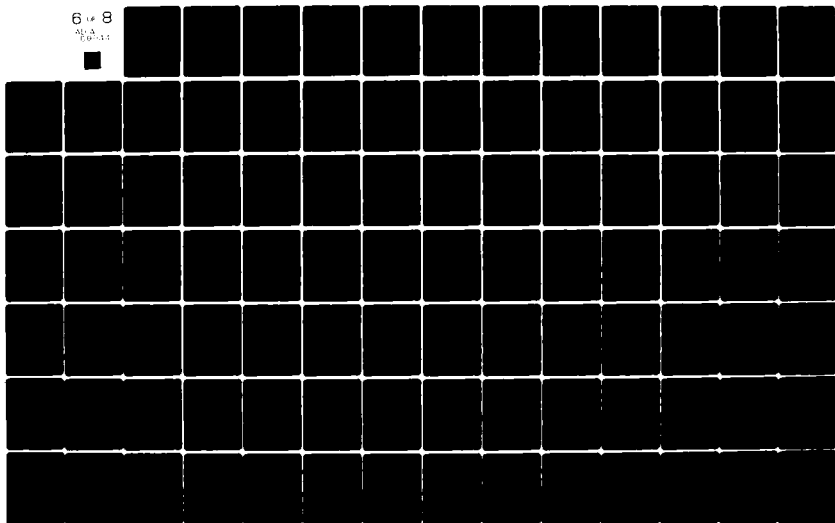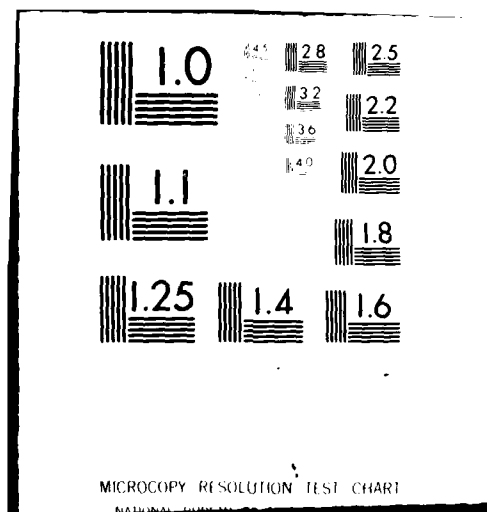
Through $\overline{M}_{\alpha_2} = (0, \alpha_2, \alpha_3^{(2)}, \ldots, \alpha_{i-1}^{(2)}, 0, \alpha_{i+1}^{(2)}, \ldots, \alpha_n^{(2)})$, let us designate small of the numbers, which separate into p_1 and p_i, in which α_2 - digit on basis/base p_2 and so on up to $\overline{M}_{\alpha_n} = (0, 0, \ldots, 0, \alpha_n)$. Let us designate through $\gamma_i^{(j)}$ the digit on basis/base p_i of number $\dfrac{\overline{M}_{\alpha_j}}{p_i}$, $(j = 1, 2, \ldots, n)$. Then, carrying out in the process of nulling the addition of digits $\gamma_i^{(j)}$ through modulus/module p_i, we obtain unknown digit γ_i.

Of course it is possible in a similar manner to obtain digit γ_i also, during the pair nulling.

Assume now we should number A divide into the product of bases/bases $p_{i_1} p_{i_2} \ldots p_{i_k} = \overline{P}$. It is possible to lead in parallel division into each of $p_{i_q} (q = 1, 2, \ldots, k)$ and to join the results of division on the basis of lemma about the division into the product of numbers. However, is feasible another path which is advisable, when the composition of the bases/bases, entering $\overline{P}$, is fixed/recorded, which occurs, for example, with the rounding. In this case the process of division into $\overline{P}$ can consist of two stages: the 1st stage - reduction of number A to the form, which separates into $\overline{P}$, i.e., nulling digits on bases/bases $p_{i_1}, p_{i_2}, \ldots, p_{i_k}$; the 2nd stage - determination of the digits of the quotient A': $\overline{P}$ from the bases/bases, entering $\overline{P}$, by nulling digits on the bases/bases, not entering $\overline{P}$.

The remaining digits A': $\overline{P}$ are obtained by step-by-step formal

division.

Let us consider the execution of these stages.

Page 292.

The 1st stage is realized on the basis of nulling number A by minimum numbers of form:

$$\overline{M}_{\alpha_{i_1}} = (\alpha_1^{(i_1)}, \alpha_2^{(i_1)}, \ldots, \alpha_{i_1}, \ldots, \alpha_n^{(i_1)})$$ - The small number, which has digit α_{i_1} on the basis/base $p_{i_1}; \ldots$

$$\overline{M}_{\alpha_{i_q}} = (\alpha_1^{(i_q)}, \alpha_2^{(i_q)}, \ldots, 0, \ldots, \alpha_{i_q}, \ldots, \alpha_n^{(i_q)})$$ - small from the numbers, which have digit α_{i_q} on basis/base p_{i_q} and multiple to product $p_{i_1}, p_{i_2}, \ldots, p_{i_{q-1}}$.

As a result of executing this stage, organized by nulling on one digit or in one step on two digits, is obtained the number
$$A' = (\beta_1, \beta_2, \ldots, 0, \ldots, 0, \ldots, \beta_n),$$
having zero in the bases/bases, entering $\overline{P}$, and least differing from A from all numbers of this form.

The 2nd stage is realized by nulling number A' by minimum numbers of following form:

$\overline{M}_{\beta_1} = (\beta_1, \ \beta_2^{(1)}, \ \ldots, 0, \ \ldots, 0, \ \ldots, \beta_n^{(1)})$ - small from numbers, multiple $\overline{P}$,

which have digit β_1 on basis/base p_1 and so forth up to

$\overline{M}_{\beta_n} = (0, 0, \ldots, 0, \ldots, \beta_n)$ - smallest of the numbers, multiple $\prod\limits_{i=1}^{n-1} p_i$, which

have digit β_n on basis/base p_n.

To each number $\overline{M}_{\beta_j}$ corresponds $\Gamma_j = (\gamma_{i_1}^{(j)}, \ \ldots, \gamma_{i_k}^{(j)})$ the number, which is

digits on the bases/bases, entering $\overline{P}$, quotient $\dfrac{\overline{M}_{\beta_j}}{\overline{P}}$.

As a result of executing this stage with nulling of digits on

the bases/bases, not entering $\overline{P}$, with the help of appropriate numbers

$\overline{M}_{\beta_j}$ is produced the addition of numbers Γ_j, which gives as a result

$\Gamma = (\gamma_{i_1}, \gamma_{i_2}, \ldots, \gamma_{i_k})$ - the number, formed by the unknown digits of quotient

$\dfrac{A'}{\overline{P}}$ on bases/bases $p_{i_1}, \ p_{i_2}, \ \ldots, p_{i_k}$. As far as digits are concerned

remaining $\dfrac{A'}{\overline{P}}$, then they, as has already been indicated, they are

formed by the formal step-by-step division of the corresponding

digits A' into ligits $\overline{P}$.

Page 293.

Let us note that this second stage is actually the variety of

the process of expanding the system of bases/bases, i.e.,

determination from the digits of a number on some preset bases/bases

of the values of its digits on any other bases/bases.

Let us consider the use/application of this method based on specific example.

Let be preset the system of the bases/bases:

$$p_1 = 3, \quad p_2 = 5, \quad p_3 = 7, \quad p_4 = 11, \quad p_5 = 13$$

with range $\mathscr{P} = 15015$.

As the divider/denominator let us select the product of bases/bases $p_3 p_4$, i.e.

$$\overline{P} = p_3 p_4 = 7 \cdot 11 = 77 = (2, 2, 0, 0, 12).$$

The minimum numbers, necessary for the nulling on bases/bases p_3 and p_4, are:

$$M_{31} = (1, 1, 1, 1, 1) \qquad M_{43} = (2, 2, 0, 3, 1)$$
$$M_{32} = (2, 2, 2, 2, 2) \qquad M_{44} = (1, 0, 0, 4, 5)$$
$$M_{33} = (0, 3, 3, 3, 3) \qquad M_{45} = (1, 4, 0, 5, 10)$$
$$M_{34} = (1, 4, 4, 4, 4) \qquad M_{46} = (1, 3, 0, 6, 2)$$
$$M_{35} = (2, 0, 5, 5, 5) \qquad M_{47} = (1, 2, 0, 7, 7)$$
$$M_{36} = (0, 1, 6, 6, 6) \qquad M_{48} = (0, 3, 0, 8, 11)$$
$$M_{41} = (2, 1, 0, 1, 4) \qquad M_{49} = (0, 2, 0, 9, 3)$$
$$M_{42} = (2, 0, 0, 2, 9) \qquad M_{410} = (0, 1, 0, 10, 8)$$

The minimum numbers, necessary for conducting the second stage are:

$$M_{11} = (1, 4, 0, 0, 11), \text{ при этом } \Gamma_{11} = (2, 2)$$
$$M_{12} = (2, 2, 0, 0, 12) \qquad \Gamma_{12} = (1, 1)$$
$$M_{21} = (0, 1, 0, 0, 10) \qquad \Gamma_{21} = (3, 3)$$
$$M_{22} = (0, 2, 0, 0, 7) \qquad \Gamma_{22} = (6, 6)$$
$$M_{23} = (0, 3, 0, 0, 4) \qquad \Gamma_{23} = (2, 9)$$
$$M_{24} = (0, 4, 0, 0, 1) \qquad \Gamma_{24} = (5, 1)$$

$$M_{51} = (0, 0, 0, 0, 1)$$
$$M_{52} = (0, 0, 0, 0, 2)$$
$$M_{53} = (0, 0, 0, 0, 3)$$
$$M_{54} = (0, 0, 0, 0, 4)$$
$$M_{55} = (0, 0, 0, 0, 5)$$
$$M_{56} = (0, 0, 0, 0, 6)$$
$$M_{57} = (0, 0, 0, 0, 7)$$
$$M_{58} = (0, 0, 0, 0, 8)$$
$$M_{59} = (0, 0, 0, 0, 9)$$
$$M_{510} = (0, 0, 0, 0, 10)$$
$$M_{511} = (0, 0, 0, 0, 11)$$
$$M_{512} = (0, 0, 0, 0, 12)$$

$$\Gamma_{51} = (6, 2)$$
$$\Gamma_{52} = (2, 4)$$
$$\Gamma_{53} = (5, 9)$$
$$\Gamma_{54} = (4, 0)$$
$$\Gamma_{55} = (4, 5)$$
$$\Gamma_{56} = (3, 7)$$
$$\Gamma_{57} = (3, 1)$$
$$\Gamma_{58} = (2, 3)$$
$$\Gamma_{59} = (2, 8)$$
$$\Gamma_{510} = (1, 10)$$
$$\Gamma_{511} = (1, 4)$$
$$\Gamma_{512} = (0, 6)$$

Key: (1). in this case.

Page 294.

Example. To divide number $A = (2, 1, 2, 3, 2)$ into the product of bases/bases $\overline{P} = p_3 p_4 = 77$.

The 1st stage. Let us lead nulling digits on bases/bases p_3 and p_4.

Nulling digit on basis/base $p_3 = 7$:.

$$A_3 = A - M_{32} = (2, 1, 2, 3, 2) - (2, 2, 2, 2, 2) = (0, 4, 0, 1, 0).$$

Nulling digit on basis/base $p_4 = 11$:.

$$A' = A_3 - M_{41} = (0, 4, 0, 1, 0) - (2, 1, 0, 1, 4) = (1, 3, 0, 0, 9).$$

As a result is obtained number A', multiple $\bar{P}$.

The 2nd stage. Obtaining the digits of the quotient

$$\frac{A'}{\bar{P}} = \frac{(1, 3, 0, 0; 9)}{(2, 2, 0, 0, 12)} .$$

Let us first of all point out the digits of quotient on the bases/bases, not entering $\bar{P}$:

$$\gamma_1 = \frac{1}{2} \pmod 3 = 2,$$

$$\gamma_2 = \frac{3}{2} \pmod 5 = 4,$$

$$\gamma_5 = \frac{9}{12} \pmod{13} = 4.$$

Let us null digit on basis/base $p_1 = 3$:

$$A_1 = A' - M_{11} = (1, 3, 0, 0, 9) - (1, 4, 0, 0, 11) = (0, 4, 0, 0, 11),$$
$$\Gamma_1 = \Gamma_{11} = (2, 2).$$

Let us null digit on basis/base $p_2 = 5$:

$$A_2 = A_1 - M_{24} = (0, 4, 0, 0, 11) - (0, 4, 0, 0, 1) = (0, 0, 0, 0, 10),$$
$$\Gamma_2 = \Gamma_1 + \Gamma_{24} = (2, 2) + (5, 1) = (0, 3).$$

Let us null digit on basis/base $p_5 = 13$:

$$A_5 = A_2 - M_{540} = 0,$$
$$\Gamma_5 = \Gamma_2 + \Gamma_{540} = (0, 3) + (1, 10) = (1, 2).$$

Final quotient

$$\frac{A'}{\bar{P}} = \frac{(1, 3, 0, 0, 9)}{(2, 2, 0, 0, 12)} = (2. 4, 1, 2, 4).$$

Page 295.

Chapter 6.

COMPONENTS OF COMPUTERS IN A SYSTEM OF RESIDUAL CLASSES.

§6.1. Adders on the arbitrary modulus/module.

In the positional numeration system the execution of arithmetic operation assumes the consecutive processing of the digits of operands according to the rules, determined by the content of this operation, and it cannot be completed until are determined consecutively/serially the values of all digits of result taking into account all connections between the digits.

In the system of residual classes each of the digits of a number is treated independently and the time of the execution of entire operation is determined by the time, necessary for obtaining of result on the greatest basis/base.

Let us consider the methodology of the construction of the adders, which work on the arbitrarily preset modulus/module, carried out on bistable elements. The use/application of the obtained results

to the elements/calls, which have is more than two steadys-state, it
can only simplify the circuit realization of the devices/equipment in
question.

Lemma 6.1. Through any cross section of adder in the process of
adding two numbers in the generalized positional numeration system
cannot pass more than one transfer.

Page 296.

Determination. The modulus/module of adder we will call minimum,
different from zero Mach numbers whose addition (or subtraction) to
the contents of adder does not vary its value, i.e.,

$$A \pm M = A, \qquad (6.1)$$

where A - contents of adder.

Let us point out the series/row of the basic properties of the
modulus/module of adder.

Property 1. In the adder with modulus/module M the result of sum
cannot exceed the modulus/module of adder.

Actually/really, let the result of the sum of two numbers A and

B exceed modulus/module M, i.e., A+B>M. Then the result of sum can be represented in the form A+B=C+M, where C<M, or in accordance with (6.1) we will obtain A+B=C<M.

Property 2. If M - modulus/module of adder, and k - arbitrary integer, then $\underset{\wedge}{A + kM = A.}$ Actually/really on (6.1)

$$A \pm kM = A \pm \underbrace{M \pm M \pm \ldots \pm M}_{k} = A.$$

Property 3. The modulus/module of adder is its second zero. Assertion follows from the determination of the modulus/module of adder.

Property 4. The adder of inverse code, which works in the polyadic positional numeration system with bases/bases $\pi_1, \pi_2, \ldots, \pi_k$, has a modulus/module M, equal

$$M = \pi_1 \pi_2 \cdots \pi_k - 1. \qquad (6.2)$$

Actually/really, addition to the contents of the adder of value $\pi_1, \pi_2 \cdots \pi_k$ is equivalent to output of unity into the feedback loop without a change in the contained adder.

Property 5. The modulus/module of the adder of the inverse code, which works in the polyadic positional numeration system with bases/bases $\pi_1, \pi_2, \ldots, \pi_k$, is the number whose digits on each of the bases/bases π_i are equal to $\pi_k - 1$ $(i = 1, 2, \ldots, k)$.

For the proof of this assertion let us consider number B,

registered in the polyadic positional numeration system in the form

$$B = (\alpha_1, \alpha_2, \ldots, \alpha_k).$$

Its value

$$B = \alpha_1 \pi_2 \pi_3 \ldots \pi_k + \alpha_2 \pi_2 \pi_4 \ldots \pi_k + \ldots + \alpha_{k-1} \pi_k + \alpha_k.$$

Page 297.

If digits α_i of the number in question are equal to $\pi_i - 1$, we will obtain

$$B = (\pi_1 - 1) \pi_2 \ldots \pi_k + \ldots + \pi_k - 1 = M.$$

In particular, for the binary number system where $\pi_1 = \pi_2 = \ldots = \pi_k = 2$, we obtain

$$M = 2^k - 1 = (1, 1, \ldots, 1, 1);$$

for the ternary system $\pi_1 = \pi_2 = \ldots = \pi_k = 3$

$$M = 3^k - 1 = (2, 2, \ldots, 2, 2)$$

and finally for the decimal system.

$$M = 10^k - 1 = (9, 9, \ldots, 9, 9).$$

Thus, binary, ternary and decimal adders have the fixed/recorded value of the modulus/module: $2^k - 1, 3^k - 1, 10^k - 1,$ which excludes the possibility of the arbitrary assignment of modulus/module and causes the following sequence of executing the operation of the addition:

a) formation/education on the adder of sum a+b;

b) the comparison of sum $\alpha + \beta$ with the value of basis/base p_i:

c) the correction of sum by subtraction p_i, if occurs relationship/ratio $\alpha + \beta \geqslant p_i$.

The sequence of similar type operations usually is realized in the arithmetic units, intended for the work in the decimal system, but constructed on the basis binary elements/cells.

Is feasible the version of the acceleration of the operation of addition due to the doubling of equipment. In this version the addition of two remainders/residues α and β is produced on two adders simultaneously: on one is implemented the operation $\alpha + \beta$, on the second $\alpha + \beta - p_i$.

In the case when on the second adder result is positive (is examined the addition of two positive remainders/residues), it is accepted for the true; if result is negative, then for the true is accepted the result, obtained in the first adder.

If the modulus/module of adder differs from the basis of system to the small value, the correction of result can be somewhat simplified.

Let us consider possible situations with the addition of two positive numbers α and β.

Page 298.

Case 1. The modulus/module of adder exceeds per one unit appropriate basis p_i of system, i.e., $M = p_i + 1$.

In this case are possible the following relationships/ratios between the result of addition and the value of the basis of the system:

a) if $\alpha + \beta < p_i$, then corrections are not required;

b) if $\alpha + \beta = p_i$, then contents of adder it is extinguished;

c) if $\alpha+\beta=M$, then in the presence of negative zero adder it is set unity into the low-order digit of adder with the simultaneous extinguishing of remaining digits;

d) if $\alpha+\beta>M$, then result of operation C it will prove to be equal to
$$C = \alpha + \beta - M = \alpha + \beta - p_i - 1 = \alpha + \beta - 1 \,(\mathrm{mod}\, p_i),$$

i.e. is less than the true per unit. In this case in the adder carry

circuit from the output/yield of the high-order digit is thrown to the input of the second digit of adder.

Case 2. The modulus/module of adder M per one unit is less than the appropriate basis p_i of system, i.e.

$$M = p_i - 1.$$

In this case appears the need in the corrections of the following character:

a) if $\alpha + \dot{\beta} < p_i$, then corrections is not required;

b) if $\alpha + \beta = p_i$, then we obtain the result, equal to +1, with the preliminary output of transfer from the high-order digit. Contents of adder is extinguished;

c) if $\alpha + \beta = M$, then the circuit of analysis to the negative zero adders extinguishes contents with the the simultaneous recording into adder -1;

d) if $\alpha + \beta > p_i$, then we obtain the result of operation of addition C in the form

$$C = \alpha + \beta - M = \alpha + \dot{\beta} + 1 \pmod{p_i},$$

i.e. is obtained the result of more than true per unit. Adder in the case in question can be carried out with extended carry circuit from

the high-order digit.

Thus, if the modulus/module of adder and the basis of system is
separated per unit, the correction of result can be realized
relatively simply.

Page 299.

The noticeable complication of correction with a difference in
the modulus/module of adder from basis/base p_i already per two units,
forces us to seek the new methods of the construction of adders,
namely in the direction of the new organization of interbit/interbyte
connections.

Let the adder consist of n of the bits, designated respectively
through $r_1, r_2, \ldots, r_n$ with an increase of the precedence of digits. Let
us agree that the input of each digit of adder will be designated by
index i, and output/yield - by index j. Let us designate through X_{ij}
the connection between output/yield r_j of digit with input r_i of the
digit of adder. Thus, the presence of connection X_{ij} ensures
connection on transfer r_j of digit not only with r_{j+1} but also with
r_i the digit. Let us consider, which of the connections X_{ij} must occur
so that the n-bit binary adder would work on modulus/module p_i, so
that would be satisfied the condition $M = p_i$. The block diagram of

adder is represented in Fig. 6.1.

Let the value of basis/base p_i be preset in the form

where
$$p_i = 2^{n-1}s_n + 2^{n-2}s_{n-1} + \ldots + 2s_2 + s_1,$$

$$s_k = 0, \ 1,$$
$$k = 1, \ 2, \ \ldots, \ n.$$

If contents of adder G_L takes the form

$$G_L = 2^{n-1}l_n + 2^{n-2}l_{n-1} + \ldots + 2l_2 + l_1,$$
where

$$l_k = 0, \ 1,$$
$$k = 1, \ 2, \ \ldots, \ n.$$

the condition of the equality the modulus/module of adder to

basis/base p_i on (6.1) will be registered in the form

$$l_i + s_i + c_{i-1} + X_{ij} = l_i,$$
$$i = 1, \ 2, \ \ldots, \ n,$$
$$(6.3)$$

where through c_i is designated the transfer from the i-th into the

i+1 digit adder or

$$s_i = c_{i-1} + X_{ij},$$
$$i = 1, \ 2, \ \ldots, \ n.$$
$$(6.4)$$
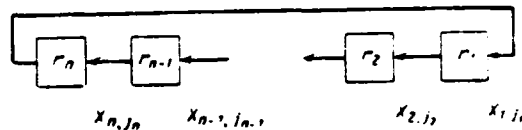
Fig. 6.1. Block diagram of adder with the additional constraints.

Page 300.

On the basis of relationship/ratio (6.4) can be formulated the following lemma.

Lemma 6.2. In "n" the discharging adder of inverse code $R\,(r_1,\,r_2,\,\ldots,\,r_n)$, which works on preset modulus/module $M = 2^{n-1}s_n + \ldots + 2s_2 + s_1$, additional constraint $X_{i,j}$ can occur only in digits r_i, which correspond to zero values $s_{i,j}$ in the digits, corresponding to single values s_{i}, additional constraints must be absent.

Determination. The weight of digit r_i of adder is called the value, which is determining, on how much is changed the numerical value of the contained adder with a change in the digit of this digit per one unit.

The given above recording

$$G_L = 2^{n-1}l_n + \ldots + 2l_2 + l_1$$

of the contained adder in the presence of additional constraints can
be used only as the symbolic indication of contents of the bits of
adder, but no longer is determined the value of number L, since the
introduction of additional constraints X_{ij} changes the weights of
single digits r_i, included by these connections, and the value of
entire number L.

To a question about the effect of one additional constraint X_{ij}
not the value of the contained adder answers the following theorem.

Theorem 6.1. Number $L = (l_1, l_2, \ldots, l_n)$, which describes contents of
the binary adder of inverse code $R = (r_1, r_2, \ldots, r_n)$, during the
introduction to one additional constraint between the output/yield of
the j digit and the input of the i digit, is reduced by value

$$\Delta G_L = 2^{i-1} \cdot \sum_{m=j+1}^{n} l_m 2 . \qquad (6.5)$$

Page 301.

Actually/really, after designating the weight of the m digit of
the adder through g_{m}, we will obtain that in the absence of additional
constraints value G_L of number L, represented on the binary adder,
will be

$$G_L = \sum_{m=1}^{n} l_m g_m.$$

where l_m - number of unity, which are contained in the m digit.

The introduction of additional constraints X_{ij} translates the numeration system of the adder in question from the binary into the polyadic whose basis are determined by the character of connections. If the basis of polyadic positional system are $\pi_1, \pi_2, \ldots, \pi_k$ and they are arranged/located in the ascending order, then unity of the m digit of number $L = (l_1, l_2, \ldots, l_k)$, represented in this system has a weight

$$g_m = \sum_{i=1}^{m-1} \pi_i.$$

Hence the value of number L is defined as

$$G_L = \sum_{m=1}^{k} l_m \prod_{i=1}^{m-1} \pi_i.$$

Let occur one additional constraint X_{ij}, which combines the output/yield of the j digit with the input of the i digit, i.e., joining the digits with numbers i, i+1, ..., j into the single digit, which works on basis/base π_{ij}. Then the weight of each digit with number j and less, it will be defined as

$$g_m = 2^{m-1},$$
$$m = 1, 2, \ldots, j.$$

The weight of digit with number j+1 and more will be defined as

$$g_m = 2^{i-1}\pi_{ij}2^{m-i-1} = 2^{m+i-j-2}\pi_{ij},$$
$$m = j+1, \ldots, n.$$

Page 302.

As can easily be seen

$$\pi_{ij} = 2^{j-i+1} - 1,$$

whence

$$g_m = 2^{m-1} - 2^{\theta}.$$

where

$$\theta = m + i - j - 2,$$

or in general form for any digit of the adder

$$g_m = 2^{m-1} - 2^{\theta}\delta_{mj},$$

where

$$\delta_{mj} = \begin{cases} 0, & \text{если } m \leqslant j, \\ 1, & \text{если } m > j, \end{cases}$$

Key: (1). if.

whence value G_L will be defined as

$$G_L = \sum_{m=1}^{n} l_m 2^{m-1} - \sum_{m=j+1}^{n} l_m 2^{\theta}.$$

At the same time in the absence of additional constraint value G_L of

number L is equal to

$$G_L = \sum_{m=1}^{n} l_m 2^{m-1},$$

i.e. with one and the same coding of number L, its value due to the introduction to one additional constraint X_i is reduced by value

$$\Delta G_L = \sum_{m=j+1}^{n} l_m 2^0 = 2^{i-j-1} \sum_{m=j+1}^{n} l_m 2^m,$$

that also composes the assertion of theorem.

Let us consider some corollaries of this.

Corollary 1. The value of number L will not be changed, if additional constraint X_{ij} is undertaken from the output/yield of the high-order digit of adder. Actually/really, with j=n we will obtain $\Delta G_L = 0$.

Corollary 2. Number $L = (l_1, l_2, \ldots, l_n)$, which describes contained n-bit adder of inverse code with one additional constraint X_{ij} can accept not more than n+i-j different numerical values, which correspond n+i-j to the possible constructions/designs of adder, which correspond to the preset modulus/module.

Actually/really, the presence of one additional constraint X_{ij} indicates that the group of (j-i+1)-th digit works on modulus/module

$\pi_{ij} = 2^{j-i+1} - 1$. Remaining n-j+i-1 digits are equal between themselves. With the transfer of any of these digits with the group, which works on modulus/module π_{ij}, the modulus/module of adder does not vary, since it is equal to

$$M = \pi_{ij}2^{n-j+i-1} - 1$$

and it does not depend on the mutual location of digits.

Page 303.

In all the possible positions of the group, which works on modulus/module π_{ij} with respect to other digits, there can be n-j+i-1. In each construction/design of adder number L, which describes its contents, will in general take the new numerical value, determined by the location of the j digit.

Let us illustrate the aforesaid based on example.

Example. Let us consider four-bit adder on modulus/module M=11. Let us introduce additional constraint $X_{3,4}$ between the output/yield of the fourth and the input of the third digit.

Version 1. j=4, i=3, n=4, π_{ij} =2^2-1=3, the modulus/module of adder $M = \pi_{ij}2^1 - 1 = 11$. The block diagram of adder is represented in Fig. 6.2.

Let with the adder be is registered number L=(1, 0, 1, 0), which for the construction/design in question has a value $G_L = 10$, which coincides with its value in the binary number system, since is satisfied condition j=n. Let us consider the remaining possible constructions/designs of adder, which work on the same modulus/module M=11.

Version 2. j=3, i=2. See *on*. Fig. 6.3. Here number value is equal to $G_L = 8$, since $\Delta G_L = 2$.

Version 3. j=2, i=1. See Fig. 6.4. Here we obtain $\Delta G_L = 2$, i.e. $G_L = 8$; the agreement of number value in the second and third versions of the constructions/designs of adder is explained by the fact that in the preset number L they took $l_3 = 0$, and then ΔG_L in both versions is identical. Thus, although a number L is preset for all cases in one and the same form, it takes different numerical values depending on the location of the group, encompassed by additional constraint.
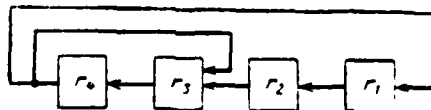
Fig. 6.2   Block diagram of adder on the Modulus/module is $\Delta G_L = 0$.
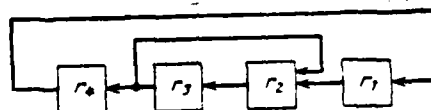
Fig. 6.3. Block diagram of adder on modulus/module 11 s
$\Delta G_L = 2$.

Page 304.

Corollary 3. The modulus/module of adder during the introduction

to one additional constraint X_{ij}, is reduced by value

$$\Delta M = 2^{i-j-2} \sum_{m=j+1}^{n} s_m 2^m,$$

where s_m - value of the m digit of a number, which describes the

value of modulus/module. Respectively by the same value is reduced

the range of the represented on the adder numbers.

Determination. By the independent additional constraints we will

understand such additional constraints, each of which contains the

group of the digits of adder, encompassed by no other additional

constraint, i.e., additional constraints X_{ij} and $X_{m,n}$ we will call

independent variables, if are satisfied the following conditions:

$$i > n$$

or   (6.6)

$$m > j.$$

For the case when on the adder is introduced s of the

independent additional constraints, can be formulated the following

theorem.

Theorem 6.2. Number $L = (l_1, l_2, \ldots, l_n)$, describing contents of the n-bit binary adder of inverse code, during introduction s of the further indepenlent connections between the outputs/yields of digits with index j_t and the input of digits with index i_t, where $t = 1, 2, \ldots, s$, is reduced by value ΔG_L where

$$\Delta G_L = \sum_{t=1}^{s} \sum_{m=j_t+1}^{j_{t+1}} l_m \sum_{\rho=1}^{t} (-1)^{\rho+1} \times$$

$$\times \sum_{\substack{q_1, q_2, \ldots, q_\rho = 1 \\ q_1 \neq q_2 \neq \ldots \neq q_\rho}}^{t} 2^{\theta_{q_1} + \theta_{q_2} + \ldots + \theta_{q_\rho} - (\rho-1)(m-1)}. \qquad (6.7)$$
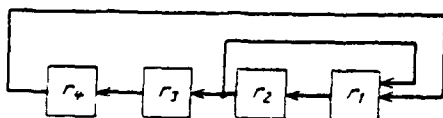
Fig. 6.4. Block diagram of adder on the modulus/module 11 $with \Delta G_L = 2$.

Page 305.

Here $\theta_q = m + i_q - j_q - 2,\ j_{s+1} = n$.

Proof. for the digits with numbers m, which satisfy the condition

$$1 \leqslant m \leqslant j_1,$$

weight it is defined as

$$g_m = 2^{m-1}.$$

For the digits, in which

$$j_1 + 1 \leqslant m \leqslant j_2,$$

the weight is equal to

$$g_m = 2^{m-1} - 2^{\theta_1},$$
$$\theta_1 = k + i_1 - j - 2.$$

For the digits whose number

$$j_2 + 1 \leqslant m \leqslant j_3,$$

weight will be defined as

$$g_m = 2^{m-1} - 2^{\theta_1} - 2^{\theta_2} + 2^{\theta_1 + \theta_2 - (m-1)}.$$

For the digits in which

$$j_3 + 1 \leqslant m \leqslant j_4,$$

as can easily be seen, weight is equal to

$$g_m = 2^{m-1} - 2^{\theta_1} - 2^{\theta_2} - 2^{\theta_3} + 2^{\theta_1+\theta_2-(m-1)} + 2^{\theta_1+\theta_3-(m-1)} + \\ + 2^{\theta_2+\theta_3-(m-1)} - 2^{\theta_1+\theta_2+\theta_3-2(m-1)}.$$

continuing this process for the digits whose numbers satisfy the condition

$$j_t + 1 \leqslant m \leqslant j_{t+1},$$

we will obtain the value of the weight

$$g_m = 2^{m-1} - (2^{\theta_1} + 2^{\theta_2} + \ldots + 2^{\theta_t}) + 2^{\theta_1+\theta_2-(m-1)} + \\ + 2^{\theta_1+\theta_3-(m-1)} + \ldots + 2^{\theta_{t-1}+\theta_t-(m-1)} - \\ - (2^{\theta_1+\theta_2+\theta_3-2(m-1)} + \ldots + 2^{\theta_{t-2}+\theta_{t-1}+\theta_t-2(m-1)}) + \ldots \\ \ldots + (-1)^\rho (2^{\theta_1+\theta_2+\ldots+\theta_\rho-(\rho-1)(m-1)} + \\ \ldots + 2^{\theta_{t-\rho+1}+\ldots+\theta_t-(\rho-1)(m-1)}) + \ldots \\ \ldots + 2^{\theta_1+\theta_2+\ldots+\theta_t-(t-1)(m-1)}, \\ \theta_t = k + i_t - i_t - 2.$$

Page 306.

Taking into account that the weight of a number on the adder without the additional constraints is defined as

$$G_L = \sum_{m=1}^{n} l_m 2^{m-1}, \qquad (6.8)$$

we will obtain the decrease of the value of number ΔG_L, coinciding with (6.7).

Example. Are preset two additional constraints

$$X_{i_1, j_1} \quad \text{and} \quad X_{i_2, j_2}, \quad \text{moreover } j_2 = n.$$

In this case

$$\Delta G_L = \sum_{m=j_1+1}^{n} l_m 2^{\theta_1},$$

where

$$\theta_1 = m + i_1 - j_1 - 2.$$

For the five-digit adder, which works on modulus/module M=17, we have

$$i_1=2, \ j_1=3, \ i_2=4, \ j_2=n=5.$$

The block diagram of adder is represented in Fig. 6.5. In accordance with (6.7) we will obtain

$$\Delta G_L = 2l_4 + 4l_5.$$

Example. Let be given three independent additional constraints on the seven-digit adder, moreover $j_3=n$. In accordance with (6.7) we have

$$\Delta G_L = \sum_{m=j_1+1}^{j_2} l_m 2^{\theta_1} + \sum_{m=j_2+1}^{n} l_m (2^{\theta_1} + 2^{\theta_2} - 2^{\theta_1 + \theta_2 - (m-1)}).$$

Fig. 6.6 depicts the block diagram of the adder, which works on modulus/module M=53. Here $i_1=2$, $j_1=3$, $i_2=4$, $j_2=5$, $i_3=6$, $j_3=n=7$, $\theta_1=m-3$, $\theta_2=m-3$.

Then

$$\Delta G_L = \sum_{m=4}^{5} l_m 2^{m-3} + \sum_{m=6}^{7} l_m (2^{m-2} - 2^{m-5}) = 2l_4 + 4l_5 + 14l_6 + 28l_7.$$

Fig. 6.5. Block diagram cf adder cn the modulus/module 17 with $\Delta G_L = 2l_4 + 4l_5$.

Page 307.

Is not deprived of interest the construction/design cf adder with the dependent additional constraints one of which contains another.

Theorem 6.3. Number $L = (l_2, l_2, ..., l_n)$, describing contents of the n-bit binary adder of inverse code, during the introduction of two additional constraints $X_{i_1 j_1}, X_{i_2 j_2}$, of those satisfying to the conditions

$$i_1 \leqslant i_2, \quad j_1 > j_2,$$

is reduced by value

$$\Delta G_L = \sum_{m=j_2+1}^{n} l_m 2^{\theta_2} + \sum_{m=j_1+1}^{n} l_m 2^{\theta_1}, \qquad (6.9)$$

where

$$\theta_t = m + i_t - j_t - 2, \quad t = 1, 2.$$

Proof. For the digits with numbers m, which lie within the limits

$$j_2 < m \leqslant j_1,$$

we will obtain

$$g_m = 2^{m-1} - 2^{\theta_2}.$$

For the digits with the numbers

$$j_1 < m \leqslant n,$$

of weight have the values

$$g_m = 2^{m-1} - 2^{\theta_3} - 2^{\theta_1}.$$

Hence, taking into account (6.8), we will obtain

$$\Delta G_L = \sum_{m=j_3+1}^{j_1} l_m 2^{\theta_3} + \sum_{m=j_1}^{} l_m (2^{\theta_3} + 2^{\theta_1}) =$$
$$= \sum_{m=j_3+1}^{n} l_m 2^{\theta_3} + \sum_{m=j_1+1}^{n} l_m 2^{\theta_1},$$

which coincides with (6.9).
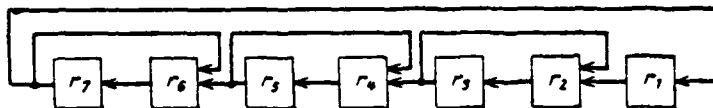
Fig. 6.6. Block diagram of the summator with respect to module 53 with $\Delta G_L = 2l_4 + 4l_5 + 14l_6 + 28l_7.$

Page 308.

Corollary. If constraint $X_{i_1 j_1}$ is connected to the high-order digit of adder, i.e., $j_1 = n$, then

$$\Delta G_L = \sum_{m=j_2+1}^{n} l_m 2^{\theta_3}.$$

Let us consider the case of three additional constraints each of which is connected with that following.

Theorem 6.4. Number $L = (l_1, l_2, \ldots, l_n)$, describing contents of the binary adder of inverse code, during the introduction of three additional constraints $X_{i_1 j_1}, X_{i_2 j_2}, X_{i_3 j_3}$, of those satisfying to the conditions

$$i_1 \leqslant i_2 \leqslant i_3,$$
$$j_1 \geqslant j_2 \geqslant j_3,$$

is reduced by value

$$\Delta G_L = \sum_{m=j_1+1}^{n} l_m 2^{\theta_1} + \sum_{m=j_2+1}^{n} l_m 2^{\theta_2} + \sum_{m=j_3+1}^{n} l_m 2^{\theta_3}. \quad (6.10)$$

Proof. For $1 \leqslant m \leqslant j_3$ we have $g_m = 2^{m-1}$, for $j_3 < m \leqslant j_2$ we will obtain $g_m = 2^{m-1} - 2^{\theta_3}$.

If $j_2 < m \leqslant j_1$, then

$$g_m = 2^{\theta_3}(2^{\theta_2-\theta_3}(2^{m-1-\theta_2}-1)-1) = 2^{m-1} - 2^{\theta_2} - 2^{\theta_3}.$$

and finally for

$$j_1 < m \leqslant n$$

occurs

$$g_m = 2^{m-1} - 2^{\theta_1} - 2^{\theta_2} - 2^{\theta_3},$$

whence for ΔG_L we obtain

$$\Delta G_L = \sum_{m=j_3+1}^{j_2} l_m 2^{\theta_3} + \sum_{m=j_2+1}^{j_1} l_m (2^{\theta_2} + 2^{\theta_3}) +$$
$$+ \sum_{m=j_1+1}^{n} l_m (2^{\theta_1} + 2^{\theta_2} + 2^{\theta_3}),$$

which coincides with (6.10).

Taking into account the uniformity of proofs, it is possible to formulate general/common/total theorem.

Page 309.

Theorem 6.5. Number $L = (l_1, l_2, \ldots, l_n)$, the describing content of the binary adder of inverse code, during introduction s of additional

constraints $X_{i_1 j_1}, X_{i_2 j_2}, \ldots, X_{i_s j_s}$, or those satisfying the condition

$$i_1 \leqslant i_2 \leqslant \ldots \leqslant i_s, \ j_1 > j_2 > \ldots > j_s,$$

is reduced by value

$$\Delta G_L = \sum_{m=j_1+1}^{n} l_m 2^{\theta_1} + \sum_{m=j_2+1}^{n} l_m 2^{\upsilon_2} + \ldots + \sum_{m=j_s+1}^{n} l_m 2^{\upsilon_s}.$$

$$(6.11)$$

Theorem is proven analogously with previous.

Example. To find the correction of the value of number ΔG_L, if connections $X_{i_1 j_1}, X_{i_2 j_2}, X_{i_3 j_3}$ satisfy the conditions

$$i_2 > i_1, \ j_1 > j_2, \ j_2 > j_1.$$

Let us first find the weight distribution of the digits:

for $1 \leqslant m \leqslant j_2$ $g_m = 2^{m-1}$;

for $j_2 < m \leqslant j_1$ $g_m = 2^{m-1} - 2^{\theta_2}$;

for $j_1 < m < j_3$ $g_m = 2^{m-1} - 2^{\theta_1} - 2^{\theta_2}$;

for $j_3 < m \leqslant n$ $g_m = 2^{m-1} - 2^{\theta_1} - 2^{\theta_2} - 2^{\theta_3} + 2^{\theta_2 + \theta_3 - (m-1)} + 2^{\theta_1 + \theta_3 - (m-1)}$.

Whence

$$\Delta G_L = \sum_{m=j_1+1}^{n} l_m 2^{\theta_1} + \sum_{m=j_2+1}^{n} l_m 2^{\theta_2} - \sum_{m=j_3+1}^{n} l_m 2^{\theta_3} -$$

$$- \sum_{m=j_3+1}^{n} l_m (2^{\theta_1} + 2^{\theta_2}) 2^{\theta_3 - (m-1)}.$$

Example. To find the correction of the value of number ΔG_L, if constraints $X_{i_1 j_1}, X_{i_2 j_2}, X_{i_3 j_3}$ satisfy the conditions

$$i_1 \leqslant i_2, \; i_3 > j_2, \; j_1 \geqslant j_3,$$

i.e. constraint $X_{i_3 j_3}$ contains independent between themselves constraints $X_{i_1 j_1}, X_{i_2 j_2}$. Let us find the weight distribution of the digits:

for $\quad 1 \leqslant m \leqslant j_2 \quad g_m = 2^{m-1}$;

for $\quad j_2 < m \leqslant j_3 \quad g_m = 2^{m-1} - 2^{\theta_2}$;

for $\quad j_3 < m \leqslant j_1 \quad g_m = 2^{m-1} - 2^{\theta_2} - 2^{\theta_3} + 2^{\theta_2 - \theta_3 - (m-1)}$;

for $\quad j_1 < m \leqslant n \quad g_m = 2^{m-1} - 2^{\theta_1} - 2^{\theta_2} - 2^{\theta_3} + 2^{\theta_2 + \theta_3 - (m-1)}$,

whence

$$\Delta G_L = \sum_{m=j_1+1}^{n} l_m 2^{\theta_1} + \sum_{m=j_2+1}^{n} l_m 2^{\theta_2} + \sum_{m=j_3+1}^{n} l_m 2^{\theta_3} - \\ - \sum_{m=j_3+1}^{n} l_m 2^{\theta_2 + \theta_3 - (m-1)}.$$

Page 310.

Example. To find the correction of the value of number ΔG_L, if constraints $X_{i_1 j_1}, X_{i_2 j_2}, X_{i_3 j_3}, X_{i_4 j_4}$ satisfy the conditions:

$$i_2 > l_1, \; j_1 > j_2, \; i_3 > l_1, \; i_4 > j_3,$$

i.e. constraint $X_{i_3 j_3}$ and $X_{i_4 j_4}$ are not depended, and constraint $X_{i_1 j_1}$ contains constraint $X_{i_2 j_2}$.

Let us find the weight distribution of the digits:

for $1 \leqslant m \leqslant j_2$ $g_m = 2^{m-1}$;

for $j_2 < m \leqslant j_1$ $g_m = 2^{m-1} - 2^{\theta_2}$;

for $j_1 < m \leqslant j_3$ $g_m = 2^{m-1} - 2^{\theta_1} - 2^{\theta_2}$;

for $j_3 < m \leqslant j_4$ $g_m = 2^{m-1} - 2^{\theta_1} - 2^{\theta_2} - 2^{\theta_3} + 2^{\theta_1 + \theta_3 - (m-1)} + {} $
$$+ 2^{\theta_2 + \theta_3 - (m-1)};$$

for $j_4 < m \leqslant n$ $g_m = 2^{m-1} - 2^{\theta_1} - 2^{\theta_2} - 2^{\theta_3} - 2^{\theta_4} + 2^{\theta_1 + \theta_3 - (m-1)} + {}$
$$+ 2^{\theta_2 + \theta_3 - (m-1)} + 2^{\theta_1 + \theta_4 - (m-1)} + {}$$
$$+ 2^{\theta_3 + \theta_4 - (m-1)} + 2^{\theta_2 + \theta_4 - (m-1)} - {}$$
$$- 2^{\theta_1 + \theta_3 + \theta_4 - 2(m-1)} - 2^{\theta_2 + \theta_3 + \theta_4 - 2(m-1)}.$$

whence

$$\Delta G_L = \sum_{m=j_1+1}^{n} l_m 2^{\theta_1} + \sum_{m=j_2+1}^{n} l_m 2^{\theta_2} + \sum_{m=j_3+1}^{n} l_m 2^{\theta_3} + {}$$
$$+ \sum_{m=j_4+1}^{n} l_m 2^{\theta_4} + \sum_{m=j_3+1}^{n} l_m 2^{\theta_1 + \theta_3 - (m-1)} + {}$$
$$+ \sum_{m=j_3+1}^{n} l_m 2^{\theta_2 + \theta_3 - (m-1)} + \sum_{m=j_4+1}^{n} l_m (2^{\theta_1 + \theta_4 - (m-1)} + {}$$
$$+ 2^{\theta_2 + \theta_4 - (m-1)} + 2^{\theta_3 + \theta_4 - (m-1)} - {}$$
$$- 2^{\theta_1 + \theta_3 + \theta_4 - 2(m-1)} - 2^{\theta_2 + \theta_3 + \theta_4 - 2(m-1)}).$$

Page 311.

§6.2. Types cf addars and the execution of operations.

Almost for each basis/base can be proposed different constructions/dasigns cf adders, which are characterized by the character of additional ccnstraints, and therefore, and the value of correction ΔG_L. Let us consider adders with $M < 100$, moreover for each of them for the purpose cf the decrease of redundancy we will choose such construction/design in which ΔG_L would be minimum.

Adder on basis/base p=3. The block diagram or adder is depicted in Fig. 6.7. The basis cf system $p = 2^2 - 1 = 3$ is realized on the binary adder without the redundancy. Additional constraints it is not required $X_{ij} = 0$. Respectively, $\Delta G_L = 0$.

Aider on basis/base p=5. The block diagram of adder is represented in Fig. 6.8. The use cf additional constraint X_{ij}, where i=2, j=3 it makes it possible tc cbtain $\Delta G_L = 0$. In this case the modulus/module of adder will te defined as

$$M = \pi_1 \pi_2 - 1 = 5.$$

since here $\pi_1 = 2$, and $\pi_2 = 2^2 - 1 = 3$.

Adder cn basis/base p=7.
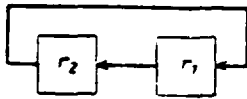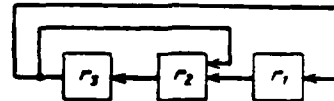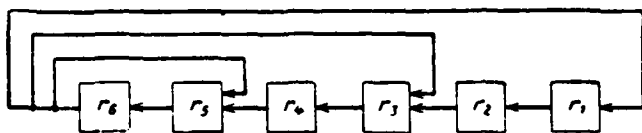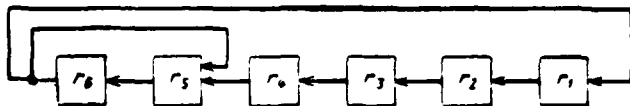
Fig. 6.7.   Fig. 6.8.

Fig. 6.7. Block diagram of adder on modulus/module 3.

Fig. 6.8. Block diagram of adder on modulus/module 5.

Page 312.

The block diagram of adder is represented in Fig. 6.9. Is used ordinary three-digit binary adder, since the basis of system $p=2^3-1=7$ on the binary adder is realized without the redundancy. In this case, is logical $X_{ij} = 0 \cdot \Delta G_L = 0$.

Adder on basis/base $p=11$. The block diagram of adder is given in Fig. 6.10. The use of additional constraint X_{ij}, where $i=3$, $j=4$, it makes it possible to obtain $\Delta G_L = 0$. In this case the modulus/module of adder will be defined as

$$M = \pi_1 \pi_2 \pi_3 - 1 = 11,$$

where $\pi_1 = \pi_2 = 2$; $\pi_3 = 2^2 - 1 = 3$.

Adder on basis/base $p=13$. The block diagram of adder is depicted

in Fig. 6.11. Is built-in additional constraint X_{ij}, where $i=2$, $j=4$.
In this case $\Delta G_L = 0$. Modulus/module of the adder

$$M = \pi_1 \pi_2 - 1 = 13,$$

where $\pi_1 = 2$; $\pi_2 = 2^3 - 1 = 7$.
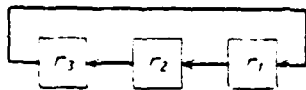
Fig. 6.9.

Fig. 6.10.

Fig. 6.9. Block diagram of adder on modulus/module 7.
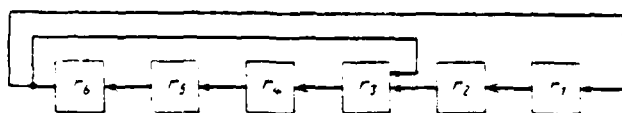
Fig. 6.10. Block diagram of adder on modulus/module 11.
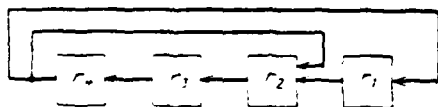
Fig. 6.11. Block diagram of adder on modulus/module 13.

Page 313.

Adder on basis/base $p=17$. The block diagram of adder is represented in Fig. 6.12. Are here introduced the additional constraints

$$X_{i_1 j_1},\ X_{i_2 j_2},\ X_{i_3 j_3}.$$

where $j_1 = j_2 = j_3 = n;\ i_1 = 2;\ i_2 = 3;\ i_3 = 4;\ \Delta G_L = 0.$

The modulus/module of adder is defined as

$$M = \{((\pi_4 \pi_3 - 1)\pi_2 - 1)\pi_1 - 1.$$

Here $\pi_4 = 2^2 - 1 = 3;\ \pi_1 = \pi_2 = \pi_3 = 2.$

If the basic criterion of the selection of constructing/designing the adder was tendency toward the decrease of a number of constraints, then it is expedient to use the diagram, depicted in Fig. 6.13. Are here introduced two additional constraints: $X_{i_1 j_1}$; $X_{i_2 j_2}$, where $i_1=2$; $j_1=3$; $i_2=4$; $j_2=5$. In this case $\Delta G_L = 4$. The modulus/module of adder is determined by value

$$M = \pi_1 \pi_2 \pi_3 - 1 = 17.$$

where $\pi_1 = 2$; $\pi_2 = \pi_3 = 2^2 - 1 = 3$.

Adder on basis/base $p=19$. The block diagram of adder is represented in Fig. 6.14. Are introduced additional constraints $X_{i_1 j_1}$, $X_{i_2 j_2}$, in which $j_1 = j_2 = 5$, $i_1 = 3$, $i_2 = 4$, thanks to which $\Delta G_L = 0$. The modulus/module of adder will be defined as

$$M = (\pi_4 \pi_3 - 1) \pi_2 \pi_1 - 1 = 19.$$

where $\pi_4 = 2^2 - 1 = 3$; $\pi_1 = \pi_2 = \pi_3 = 2$.
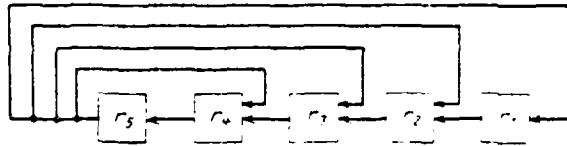
Fig. 6.12. Block diagram of adder on modulus/module 17.

Fig. 6.13. Block diagram of adder on modulus/module 17.

Page 314.

Adder on basis/base $p=23$. The block diagram of adder is given in Fig. 6.15. Is built-in additional constraint X_{ij}, where $i=4$, $j=5$, in consequence of which we obtain $\Delta G_L = 0$ and the modulus/module of the adder

$$M = \pi_1\pi_2\pi_3\pi_4 - 1 = 23.$$

Here $\pi_4 = 3$; $\pi_1 = \pi_2 = \pi_3 = 2$.

Adder on basis/base $p=29$. The block diagram of adder is given in Fig. 6.16. Is introduced additional constraint X_{ij}, where $i=2$, $j=5$, thanks to which $\Delta G_L = 0$ and the modulus/module of the adder

$$M = \pi_1\pi_2 - 1 = 29,$$

where $\pi_2 = 2^4 - 1 = 15$; $\pi_1 = 2$.

Adder on basis/base $p=31$. The block diagram of adder is depicted in Fig. 6.17. Binary five-digit adder with the feedback works on modulus/module $M = 2^5 - 1 = 31$ with correction $\Delta G_L = 0$.
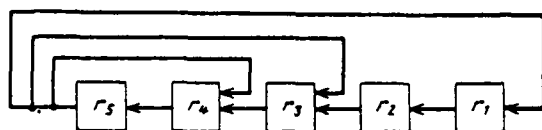
Fig. 6.14. Block diagram of adder on modulus/module 19.
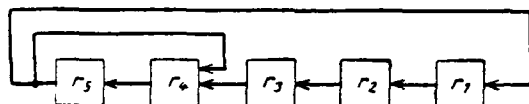
Fig. 6.15. Block diagram of adder on modulus/module 23.
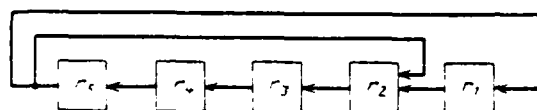
Fig. 6.16. Block diagram of adder on modulus/module 29.

Page 315.

Adder on base p=37. The block diagram of adder is represented in Fig. 6.18. Adder can be carried out by the addition of one bit to the adder, which works on modulus/module 19, and by the inclusion/connection of feedback. Then the modulus/module of adder is defined as

$$M = \pi_1\pi_2 - 1 = 37,$$

where $\pi_2 = 19$; $\pi_1 = 2$; $\Delta G_L = 0$.

Adder on basis/base p=41. The block diagram of adder is given in Fig. 6.19. Are introduced additional constraints $X_{i_1 j_1}$, $X_{i_2 j_2}$, $X_{i_3 j_3}$, moreover $j_1 = j_2 = j_3 = 6$, $i_1 = 2$, $i_2 = 3$, $i_3 = 5$. In consequence of which $\Delta G_L = 0$ and the modulus/module of the adder

$$M = ((\pi_5\pi_4\pi_3 - 1)\pi_2 - 1)\pi_1 - 1 = 41$$

with $\pi_5 = 3$, $\pi_1 = \pi_2 = \pi_3 = \pi_4 = 2$.

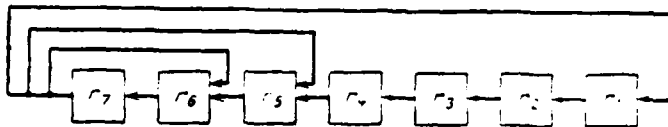Fig. 6.17. Block diagram of adder on modulus/module 31.
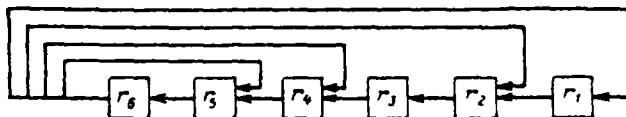
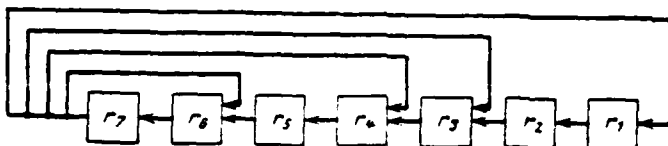Fig. 6.18. Block diagram of adder on modulus/module 37.
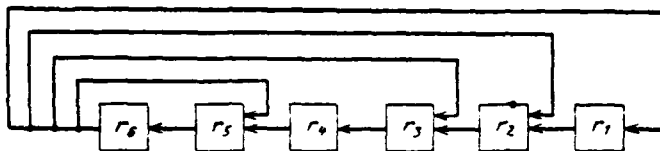
Fig. 6.19. Block diagram of adder on modulus/module 41.

Page 316.

Adder on basis/base p=43. Block diagram of the adder is shown in Fig. 6.20. Are built-in additional constraints $X_{i_1 j_1}$ and $X_{i_2 j_2}$, where $j_1 = j_2 = 6$; $i_1 = 3$; $i_2 = 5$. In this case the modulus/module of adder is equal to

$$M = (\pi_5 \pi_4 \pi_3 - 1) \pi_2 \pi_1 - 1 = 43,$$

where $\pi_5 = 2^2 - 1 = 3$; $\pi_1 = \pi_2 = \pi_3 = \pi_4 = 2$.

Adder on basis/base p=47. The block diagram of adder is represented in Fig. 6.21. Additional constraint X_{ij}, where i=5, j=6, ensures $\Delta G_L = 0$. In this case the modulus/module of adder will be

$$M = \pi_5 \pi_4 \pi_3 \pi_2 \pi_1 - 1 = 47$$

with $\pi_5 = 3$, $\pi_1 = \pi_2 = \pi_3 = \pi_4 = 2$.

Adder on basis/base p=53. The block diagram of adder is represented in Fig. 6.22. Are introduced two additional constraints $X_{i_1 j_1}$, $X_{i_2 j_2}$, in which $j_1 = j_2 = 6$, $i_1 = 2$; $i_2 = 4$.

Fig. 6.20. Block diagram of adder on modulus/module 43.
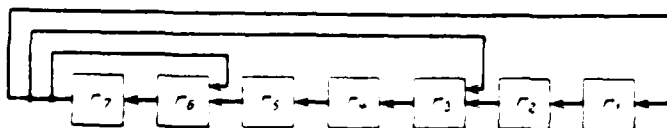

Fig. 6.21. Block diagram of adder on modulus/module 47.
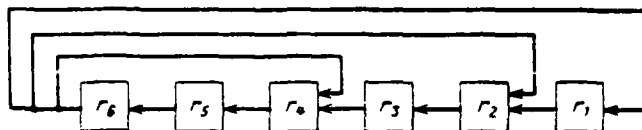
Fig. 6.22. Block diagram of adder on modulus/module 53.

Page 317.

In this case $\Delta G_L = 0$ and the modulus/module of adder will be defined as

$$M = (\pi_4 \pi_3 \pi_2 - 1) \pi_1 - 1 = 53,$$

where $\pi_4 = 2^3 - 1 = 7$; $\pi_1 = \pi_2 = \pi_3 = 2$.

Adder on basis/base $p = 59$. The block diagram of adder is given in Fig. 6.23. Is introduced additional constraint X_{ij}, in which $i = 3$, $j = 6$, thanks to which $\Delta G_L = 0$ and the modulus/module of the adder

$$M = \pi_3 \pi_2 \pi_1 - 1 = 59$$

with $\pi_3 = 2^4 - 1 = 15$, $\pi_1 = \pi_2 = 2$.

Adder on basis/base $p=61$. The block diagram of adder is given in Fig. 6.24. Occurs one additional constraint X_{ij} with $i=2$, $j=6$. In this case $\Delta G_L=0$ and the modulus/module of the adder

$$M = \pi_1 \pi_2 - 1 = 61$$

with $\pi_2 = 2^5 - 1 = 31$; $\pi_1 = 2$.

Adder on basis/base $p=67$. The block diagram of adder is represented in Fig. 6.25. Occur four additional constraints: $X_{i_1 j_1}$, $X_{i_2 j_2}$, $X_{i_3 j_3}$, $X_{i_4 j_4}$, where $j_1 = j_2 = j_3 = j_4 = 7$; $i_1 = 3$; $i_2 = 4$; $i_3 = 5$; $i_4 = 6$, thanks to which $\Delta G_L = 0$ and the modulus/module of adder is determined

$$M = (((\pi_6 \pi_5 - 1)\pi_4 - 1)\pi_3 - 1)\pi_2 \pi_1 - 1 = 67,$$

where $\pi_6 = 3$; $\pi_1 = \pi_2 = \pi_3 = \pi_4 = \pi_5 = 2$.

Fig. 6.23. Block diagram cf adder cn modulus/module 59.
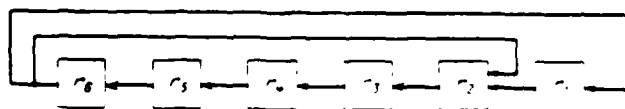
Fig. 6.24. Block diagram cf adder cn modulus/module 61.

Page 318.

The same modulus/module can te realized cn the adder, represented in Fig. 6.26, but fcr it $\Delta G_L = 16$.

Adder on basis/base $p=71$. The block diagram of adder is given in Fig. 6.27. Adder has three additicnal constraints: $X_{i_1 j_1}$, $X_{i_2 j_2}$, $X_{i_3 j_3}$, in which $j_1 = j_2 = j_3 = 7$, $i_1 = 4$, $i_2 = 5$, $i_3 = 6$, $\Delta G_L = 0$ and modulus/module is equal to

$$M = ((\pi_6 \pi_5 - 1) \pi_4 - 1) \pi_3 \pi_2 \pi_1 - 1 = 71,$$

where $\pi_6 = 3$; $\pi_1 = \pi_2 = \pi_3 = \pi_4 = \pi_5 = 2$.

Adder on basis/base $p=73$. The block diagram of adder is given in Fig. 6.28. Adder has four additioral constraints and modulus/module, characterized by the relationships/ratios

$$j_1 = j_2 = j_3 = j_4 = 7, \ i_1 = 2, \ i_2 = 3, \ i_3 = 5, \ i_4 = 6, \ \Delta G_L = 0;$$
$$M = (((\pi_6 \pi_5 - 1) \pi_4 \pi_3 - 1) \pi_2 - 1) \pi_1 - 1 = 73,$$
$$\pi_6 = 3, \ \pi_1 = \pi_2 = \pi_3 = \pi_4 = \pi_5 = 2.$$
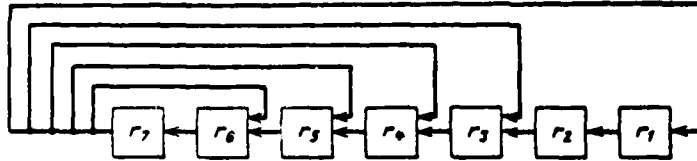
Fig. 6.25. Block diagram of adder on the modulus/module 67 with $\Delta G_L = 0$.
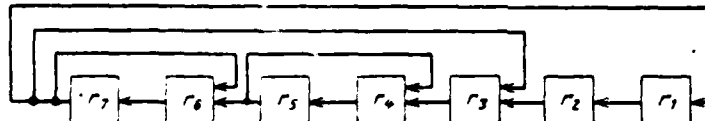
Fig. 6.26. Block diagram of adder on modulus/module 67 with $\Delta G_L = 16$.
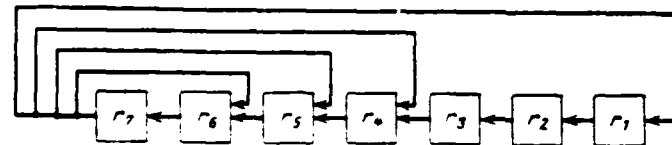
Fig. 6.27. Block diagram of adder on modulus/module 71.

Page 319.

Adder on basis/base $p=79$. Adder circuit is represented in Fig. 6.29. Occur two additional constraints: $X_{i_1 j_1}$, $X_{i_2 j_2}$, moreover $j_1 = j_2 = 7$, $i_1 = 5$, $i_2 = 6$. In this case $\Delta G_L = 0$ and the modulus/module of adder will be defined as

$$M = (\pi_6 \pi_5 - 1)\,\pi_4 \pi_3 \pi_2 \pi_1 - 1 = 79$$

with $\pi_6 = 3$, $\pi_1 = \pi_2 = \pi_3 = \pi_4 = \pi_5 = 2$.

Adder on basis/base $p=83$. The block diagram of adder is represented in Fig. 6.30. Are realized three additional constraints:

$X_{i_1 j_1}$, $X_{i_2 j_2}$, $X_{i_3 j_3}$ where $j_1 = j_2 = j_3 = 7$; $i_1 = 3$; $i_2 = 4$; $i_3 = 6$; thanks to which $\Delta U_L = 0$ and the modulus/module of adder will be defined as

$$M = ((\pi_6 \pi_5 \pi_4 - 1) \pi_3 - 1) \pi_2 \pi_1 - 1 = 83$$

with $\pi_6 = 3$, $\pi_1 = \pi_2 = \pi_3 = \pi_4 = \pi_5 = 2$.

Fig. 6.28. Block diagram cf adder cn modulus/module 73.

Fig. 6.29. Block diagram cf adder cn modulus/module 79.

Fig. 6.30. Block diagram cf adder cn modulus/module 83.

Page 320.

Adder cn basis/base p=89. The block diagram of adder is given in Fig. 6.31. It is realized by three additional constraints: $X_{i_1j_1}$, $X_{i_2j_2}$, $X_{i_3j_3}$, where $j_1=j_2=j_3=7$; $i_1=2$; $i_2=\frac{3}{4}$ $i_3=6$. In this case $\Delta G_L=0$, and the modulus/module of adder is determined

$$M = ((\pi_6\pi_5\pi_4\pi_3 - 1)\,\pi_2 - 1)\,\pi_1 - 1 = 89,$$

where $\pi_6 = 3;\ \pi_1 = \pi_2 = \pi_3 = \pi_4 = \pi_5 = 2.$

Adder on basis/base p=91. The block diagram of adder is represented in Fig. 6.32. For the realization of adder it is sufficient two additional constraints; $X_{i_1j_1}, X_{i_2j_2}$,   moreover

$j_1 = j_2 = 7$, $\mathfrak{z}_1 = 3$, $i_2 = 6$. Then $\Delta G_\mathsf{L} = 0$ and the modulus/module of adler is equal to

$$M = (\pi_6 \pi_5 \pi_4 \pi_3 - 1) \pi_2 \pi_1 - 1 = 91$$

with $w_6 = 3$; $w_1 = w_2 = w_3 = w_4 = w_5 = 2$.

Fig. 6.31. Block diagram of adder on modulus/module 89.

Fig. 6.32. Block diagram of adder on modulus/module 91.

Fig. 6.33. Block diagram of adder on modulus/module 97.

Page 321.

Adder on basis/base p=97. The block diagram of adder is represented in Fig. 6.33. For the realization of adder it is necessary to introduce four additional constraints: $X_{i_1 j_1}, X_{i_2 j_2}, X_{i_3 j_3}, X_{i_4 j_4}$ in which $j_1=j_2=j_3=j_4=7$, $i_1=2$, $i_2=3$, $i_3=4$, $i_4=5$. Then $\Delta G_L = 0$, and the modulus/module of adder is determined by value

$$M = (((\pi_5 \pi_4 - 1)\pi_3 - 1)\pi_2 - 1)\pi_1 - 1 = 97$$

with $\pi_5 = 7$, $\pi_1 = \pi_2 = \pi_3 = \pi_4 = 2$.

As the illustration let us satisfy the addition of two numbers
on the adder with modulus/module M=53.

Example. To sum the numbers

$$x = 42 = 101010$$

and

$$\beta = 45 = 101101$$

on the adder, which works on modulus/module M=53.

<div>

	101010
	101101
(1)Поразрядная сумма	000111
(2)Выход переноса	1 1
(3)Занесение переноса	11 11
(4)Суммирование поразрядной суммы с переносами	100010

</div>

Key: (1). Step-by-step sum. (2). Carry output. (3). Recording of
transfer. (4). Addition of step-by-step sum with transfers.

Is obtained the result of addition $x+\beta=100010=34$. Actually/really:
$x+\beta=87 \pmod{53}=34$.

Let us consider the execution of the operation of subtraction on
the adder of inverse code with additional constraints.

Usually the operation of the subtraction of a number β from a
number x on the adders is implemented by the addition of a number x
with the addition of a number β to the modulus/module of adder, i.e.

$$\alpha - \beta = \alpha + \bar{\beta},$$

where

$$\bar{\beta} = M - \beta.$$

On the binary adders without the additional constraints the addition of a number β to the value of the modulus/module of adder is realized simply by the inversion of a number β.

The introduction of additional constraints translates adder, as it was shown earlier, into the polyadic numeration system with bases/bases $\pi_1, \ldots, \pi_\lambda$, where the inversion of a number differs somewhat from its addition to the modulus/module.

Page 322.

The fact is that the inversion of the digit, undertaken on basis/base π_i, is the formation/education of addition to π_i, while we should have an addition from $\pi_i - 1$. In other words, the inversion of the digits, included by additional constraints, exceeds the addition of digits on their modulus/module per unit, whereas the inversion of the digits, not encompassed by additional constraints, coincides with their addition to the modulus/module. Hence the addition of a number can be obtained as follows:

- on the additional constraints of adder is adjoined unity;

- obtained code is inverted.

In the adders in which requirement $\Delta G_L = 0$, the addition of unity is exposed/persistently facilitated by the fact that the additional constraints usually proceed only from the high-order digit. Hence the addition of unity according to the additional constraints is equivalent to the imitation of transfer from the high-order digit.

Let us consider the execution of the operation of subtraction on the adder, which works on modulus/module M=53.

Example. To subtract from a number α a number β, if $\alpha=47=101111$, $\beta=25=011001$. Let us compute value of β_1, which is obtained after addition to a number of unity, according to the additional constraints

$$\beta = 011001$$
$$\frac{1\ \ 1}{}$$
$$\beta_1 = \overline{100011}$$

Let us find by inversion the addition $\bar{\beta}$ of a number β: $\bar{\beta}=011100$.

Let us find the difference

$$\alpha - \beta = \alpha + \bar{\beta} = 101111 + 011100 = 010110 = 22.$$

Actually/really, $\alpha-\beta=47-25=22$. The operation of subtraction $\beta-\alpha$, with which the minuend is lower than the subtrahend, must give the addition of a number $\alpha-\beta>0$ to the modulus/module of adder.

An example. To subtract from a number β a number α, if $\alpha=47=101111$, $\beta=25=011001$.

Let us compute value α_1, which is obtained after addition to a number α of unity, according to the additional constraints

$$\begin{array}{r} \alpha = 101111 \\ 1\ 1 \\ \hline \alpha_1 = 111001 \end{array}$$

Let us find the inversion of a number α: $\bar{\alpha}=000110$. Actually/really, $\bar{\alpha}=6=53-47$.

Let us find the result of subtraction $\beta-\alpha$

$$\beta-\alpha=\beta+\bar{\alpha}=011001+000110=011111, \text{ i.e. } \beta+\bar{\alpha}=31.$$

Actually/really,

$$\beta-\alpha=25-47=53+25-47=31.$$

Page 323.

Let us consider the execution of the operation of multiplication on the adder with $\Delta \dot{G}_L = 0$.

Let us designate through α and β, correspondingly, the multiplicand and the multiplier,

$$\alpha = 2^{n-1}a_n + 2^{n-2}a_{n-1} + \ldots + 2a_2 + a_1,$$
$$\beta = 2^{n-1}b_n + 2^{n-2}b_{n-1} + \ldots + 2b_2 + b_1.$$

Then the product of operands is defined as

$$\alpha\beta = (\alpha 2^{n-1})\,b_n + (\alpha 2^{n-2})\,b_{n-1} + \ldots + (\alpha 2)\,b_2 + \alpha b_1.$$

When $\Delta G_L = 0$ we work with the binary code whose value completely corresponds to the weights of the bits, so that the shift/shear of a number to the left, if it does not appear transfer from the high-order digit, is equivalent to multiplication by the binary basis/base, while in the presence of transfer result is corrected to the value, equal to the modulus/module of adder. It should be noted that both with the operations of addition and subtraction and with the execution of shift/shear on the adder with the additional constraints is possible the formation/education of the result, which differs from the unknown by value modulus/module of adder.

Actually/really, in accordance with special features/peculiarities examined above of the modulus/module of adder, the latter is represented in the form $\prod_{i=1}^{k} \pi_i - 1$ for i=1, 2, ..., k. Since the modulus/module is the second zero adders, its presence assumes the extinguishing of elementary adder with the output of unity of the transfer into the more high-order digit.

Naturally the report/event indicated cannot be carried out, since transfer can be caused only by the number, which exceeds modulus/module at least per unit.

It is here interesting to note that the construction/design of adder with $\Delta G_L = 0$, performed by the introduction of additional constraints from the output/yield of the high-order digit of adder, entity of the limitation indicated does not vary. Actually/really, reducing of additional constraints to the high-order digit of adder permits to expect for correction on the modulus/module only, if contents of adder exceeds value $2^n - 1$, i.e. they can take place $2^n - 1 - M$ of those not corrected on modulus/module M of results of operation.

Page 324.

The advantage of the fulfillment of the operation of multiplication on the adder with additional constraints, is defined by the fact that on it is required one correction of final result, and the others are implemented automatically on preset modulus/module p_i, while on the adder where are absent additional constraints, it will be required in the worse case

$$\left[\frac{(p_i - 1)(p_i - 1)}{p_i} \right] = p_i - 2$$

of corrections. In this case grows respectively the discharge/digital configuration of adder.

As the illustration let us give an example of the multiplication of numbers on the adder, which works on modulus/module $M = 19$.

Example. To compute product $\alpha\beta$, where the multiplicand $\alpha=13=01101$; and multiplier $\beta=15=01111$.

Since the low-order digit of the multiplier zero, to the adder will be brought in multiplicand 01101. Further multiplicand is shifted/sheared to one digit to the left, i.e., $2\alpha=11010$.

Since the second digit zero, the moved one digit multiplicand is adjoined to the contents of adder.

[1] Содержимое сумматора	0 1 1 0 1
[2] Сдвинутое множимое 2α	1 1 0 1 0
	0 0 1 1 1
[3] Занесение переноса через дополнительные связи	1 1 1
[4] Частичное произведение	1 0 1 0 0

Key: (1). Contents of adder. (2). Moved multiplicand 2α. (3). Recording of transfer through additional constraints. (4). Partial product.

The third digit of multiplier is also different from zero. In connection with this to the contents of adder must be adjoined the multiplicand, moved to the left one more digit, i.e., $2^2 \cdot \alpha$.

[1] При этом $2^2 \cdot \alpha$	1 0 1 0 0
[2] Занесение переносов	1 1 1
	0 0 0 0 1
[3] Повторное занесение переносов	1 1 1
[4] Результат	0 1 1 1 0

Key: (1). In this case $2^2 \cdot \alpha$. (2). Recording of transfers. (3).
Repeated recording of transfers. (4). Result.

Let us count the next sum of partial products.

(1) Частичное произведение	1 0 1 0 0
(2) Сдвинутое множимое	0 1 1 1 0
	0 0 0 1 0
(3) Занесение переносов	1 1 1
(4) Частичное произведение	0 1 1 1 1

Key: (1). Partial product. (2). Moved multiplicand. (3). Recording of
transfers. (4). Partial product.

Fourth digit of the multiplier zero. Let us find $2^3 \cdot \alpha = 11100$. Let us
compute the partial product

	0 1 1 1 1
	1 1 1 0 0
	0 1 0 1 1
(1) Занесение переносов	1 1 1
	1 1 0 0 0

Key: (1). Recording of transfers.

Page 325.

Thus, was obtained the result

$$\alpha\beta = 11000 = 24 = 5 \,(\text{mod } 19).$$

Actually/really, result is accurate, since by testing in the decimal
system we obtain

$$\alpha\beta = 13 \cdot 15 = 195 = 5 \,(\text{mod } 19).$$

Given earlier lemma 6.1, which claims that through any cross section of binary adder with the addition of two numbers cannot pass more than one transfer, for the adder with the additional constraints, which works on the arbitrarily preset modulus/module, is in general not applied.

The process of addition on this adder of two numbers α and β, which satisfy condition $\alpha < M$, $\beta < M$, consists of the following operations:

- step-by-step addition of numbers A and B with the formation/education of transfers;

- addition of step-by-step sum with the obtained transfers;

- addition of the obtained result with the transfers of further circuits X_{ij} and feedback loop in the presence of transfer from the output/yield of the high-order digit of adder.

On a number of possible transfers for the adders with the additional constraints can be formulated the following lemmas.

Lemma 6.3. Through any cross section of adder with s additional constraints X_{ij}, working on modulus/module M and with $\Delta G_L = 0$, in the

process of adding two numbers α and β, which satisfy the condition

$$\alpha < M, \ \beta < M, \qquad (6.12)$$

Can pass not more than two transfers and cannot take the place of more than one transfer from the output/yield of the high-order digit of adder.

$$(\alpha + \beta)_{max} = 2M - 2.$$

Proof. On (6.12) the greatest possible sum takes the form

From the high-order digit more than one transfer leave cannot, since after carry output contents of adder G_L is reduced by value

$$\Delta G_L = 2^n - 1 - \sum_{i=1}^{s} X_{ij} g_i.$$

Page 326.

Here g_i - weight of the group of the digits, included by constraint X_{ij}, and in the extreme case G_L is equal

$$G_L = 2M - 1 - 2^n + \sum_{i=1}^{s} X_{ij} g_i.$$

Let us consider now how is changed the modulus/module of single polyadic digits and entire adder upon inclusion/connection of s additional constraints, which begin from the high-order digit of adder. The modulus/module of the digits of adder, included by low-order additional constraint X_{in}, is equal to

$$M^{(1)} = 2^{n - i_1 + 1} - 1.$$

Upon the inclusion/connection of following on the precedence connection X_{2n} we will obtain the modulus/module

$$M^{(2)} = 2^{n - i_2 + 1} - 1 - 2^{i_1 - i_2}.$$

Upon the inclusion/connection of the third connection

$$M^{(3)} = 2^{n - i_3 + 1} - 1 - 2^{i_1 - i_3} - 2^{i_2 - i_3},$$

. . . .

Upon the inclusion/connection of connection with number s we will obtain the modulus/module

$$M^{(s)} = 2^{n - i_s - 1} - 1 - 2^{-i_s} \sum_{k=1}^{s-1} 2^{i_k},$$

. . . .

The total modulus/module of adder with the feedback will be equal to

$$M = 2^n - 1 - 2^{i_s - 1} - 2^{-1} \sum_{k=1}^{s-1} 2^{i_k}. \qquad (6.13)$$

Taking into account that in the case

$$\sum_{i=1}^{s} X_{ijgl} = \sum_{k=1}^{s} 2^{i_k-1}$$

in question from (6.12) and (6.13), we will obtain

$$G_L = 2^n - 3 - \sum_{k=1}^{s} 2^{i_k-1} < 2^n.$$

i.e. the second transfer from the high-order digit is impossible.

Page 327.

Any digit of adder participates maximum in two additions. One of them - this is the addition of operands, the second - addition with the code according to the additional constraints, since the code according to the additional constraints enters the addition not more than one time. But with each summation is feasible only the one transfer through the cross section of adder, that also proves the assertion of lemma.

On a number of possible transfers in the case of uncorrected operands can be formulated the following lemma.

Lemma 6.4. Through any cross section of n-bit adder with the additional constraints, connected to the high-order digit of adder, in the process of adding two numbers α and β, that satisfy the condition $\alpha \leqslant 2^n - 1, \beta \leqslant 2^n - 1,$

can pass not more than three transfers and not more than two transfers can leave the high-order digit of adder.

Proof. Actually/really, let us consider the case of the addition of greatest numbers $\alpha = 2^n - 1$, $\beta = 2^n - 1$, whose sum $\alpha + \beta = 2^{n+1} - 2$. The minimum modulus/module, realized on the n-bit adder, obviously, is not less 2^{n-1}, since for the realization of a modulus/module less even per unit, it would be sufficient have (n-1)-digit adder.

But then already in the presence of two transfers from the high-order digit, contents of adder will be $G_L = 2^n - 2$ and the third transfer from the high-order digit of adder is impossible. On the strength of the fact that the adder participates in three additions, a quantity of transfers in the cross section of adder cannot be more than three.

§6.3. Bases of tabular arithmetic.

Determination. By the tabular realization of the relationship/ratio

$$z_i = f(x_i, y_i) \qquad (6.14)$$

let us agree to understand the organization of such table in which to each combination of input values x_i and y_i corresponds one and only one value of output quantity z_i.

It is logical that the access to such a table in terms of values x_i and y_i assumes appearance at its output/yield of value z_i.

The idea of the use of tables in the computers is not new. In the storage of machines are built-in the tables of the values of initial values, table of different constants, values of elementary functions, etc.

Page 328.

There are many circuit embodiment of the tables, which realize these or other logical functions. For example, the widespread schematic of decoder for the n-bit binary code realizes 2^n the possible combinations of the codes. With the more general/more common/more total approach to the schematic of decoder, assuming the realization of any possible binary combination at its 2^n outputs/yields, we will obtain 2^{2^n} different output functions. In this case, naturally, will not be withstood the one-to-one correspondence between the number of combinations of input values x_i and y_i with output z_i, but value 2^{2^n} characterizes the functional completeness of decoder diagram.

Studying questions of machine arithmetic, we will be, in

essence, interested in the tabular realization of relationship/ratio (6.14), on the basis of the fact that x_i, y_i, z_i for all possible values of i are whole non-negative numbers.

[0, X) - the range of a change in value x_i;

[0, Y) - the range of a change in value y_i;

[0, Z) - the range of a change in value z_i.

Then a number of possible mutual combinations x_i and y_i will be defined as by XY. The condition for one-to-one correspondence $x_i y_i$ to values z_i will determine the requirement

$$Z < XY. \qquad (6.15)$$

Assuming subsequently, that the values of input values lie/rest at one range [0, X), we will obtain $Z \leqslant X^2$.

Determination. By redundancy $\mathcal{J}$ of table we will understand the difference between a number of possible combinations of input values and number of the permissible values of output function, i.e.

$$\mathcal{J} = X^2 - Z. \qquad (6.16)$$

The redundancy of table directly characterizes its design concept and indirectly its electrical parameters. If $Z < X^2$, then this means that sets XY and Z are not one-to-one, i.e., to this combination x_i, y_i

corresponds one and only one value z_i, and to this value z_i can correspond not only one combination x_i and y_i. In this case can be set the task about the selection of constructing/designing the table, which will make it possible maximally to decrease a quantity of duplicated/backed up/reinforced results.

Page 329.

Determination. By j assembly let us agree to understand the part of the table, which realizes relationship/ratio $z_j = f(x_j, y_j)$.

Obviously, in general a number of assemblies of table will be defined as $N = X^2$. This is correct, when is realized each possible combination of input values, and then the outputs/yields of assemblies are joined according to the rules, determined by the form of the function f. Function f characterizes contents of operation, while sets X and Y determine the ranges of input values and from the content of operation they do not depend.

Determination. By coefficient of the use of table let us agree to understand the expressed in the percentages ratio of a quantity of possible output values to a quantity of assemblies of table, i.e.

$$v = \frac{Z}{N} 100\%. \qquad (6.17)$$

Value w, reciprocal to the coefficient of use, we will call the

coefficient of redundancy, i.e.

$$\omega = \frac{N}{Z} \, 100\%. \qquad (6.18)$$

Let us consider for an example of the characteristic of table, which realizes two-component operation in the binary positional numeration system. Operands x_i, y_i and values of possible results of operation lie/rest in the range $[0, X)$, where $X = 2^n$. Hence a number of possible combinations of input values or, which is the same, a number of assemblies of table will be defined as $N = X^2 = 2^{2n}$. But possible results of operation lie/rest at the same range, as initial values. Hence the redundancy of table will be

$$\mathcal{J} = 2^n (2^n - 1).$$

The coefficient of use is defined as

$$\nu = \frac{100}{2^n} \% \approx 2^{7-n} \%,$$

the coefficient of redundancy

$$\omega \approx 2^{n-7} \%.$$

As we see, the characteristics of tables are exponential functions from a number of input. Therefore the execution of arithmetic operations in the positional machines by purely tabular methods realized up to now in view of an enormous quantity of required equipment.

Page 330.

Actually/really, if we consider the arithmetic unit, which works in

the binary positional numeration system and which uses, for example, with 30-digit numbers, i.e., n=30, then for the tabular realization of any operation will be required table with a number of assemblies $N=2^{60} \approx 10^{18}$. Its redundancy also will be defined as $J \approx 10^{18}$. The coefficient of utilization will be $v=10^{-9}\%$, i.e., it will be necessary to construct the in practice unrealizable construction which will be used by 10^{-9} percent.

Qualitatively different results we will obtain upon transfer to the system of residual classes. For the realization of the same range on the order of 2^{30} or 10^9 to us to sufficient use a system of bases/bases 3, 7, 11, 13, 17, 19, 23, 25, 29, greatest of which requires for the storage 5-bit binary register.

For the realization of operations on the greatest basis p=29 of numeration system in question is required the table, whose input and output data vary in the range [0, 29), i.e., a number of assemblies of such table will be defined as $N=29^2=841$, and the coefficient of its use will be $v=\frac{100}{29}\%=3,3\%$. For the realization of operations on the smallest basis/base p=3 will be required the table with a number of assemblies $N=3^2=9$, and the coefficient of the use of this table will be defined as $v=\frac{100}{3}\% \approx 33,3\%$.

The given above calculations of the characterizing table values

are given in the most general/most common/most total plan/layout,
without the account to the commutation of input, which for the
majority of operations occurs, without the account to the possibility
of using special coding, the organization of work in the second
step/stage, etc. Subsequently let us see, that the enlistment of this
further information can substantially improve construction/design and
characteristics of table.

From that stated above it is evident that the questions,
connected with the execution of arithmetic operations by tabular
methods, it is expedient to examine only in application to the
arithmetic units, which work in the residual classes.

Further, the series/row of the operations, realized by
arithmetic ones by device/equipment, does not require the
use/application of two-input tables. For example, the realization of
such functions as e^x, ln x, all trigonometric functions, the
calculation of the value of polynomial with the constant
coefficients, etc., requires the use only of the single-input tables
whose construction/design is significantly simpler than two-input.

Page 331.

In them we deal concerning one argument, which are changed in the

range [0, X) and, naturally, is implemented only the number of
assemblies of tables which is intended for the realization of output
quantities z_i from the range [0, Z). Here almost always N=Z. In this
case are obtained redundancy $y = 0$, coefficient of use $v = 100\%$.
Therefore subsequently it is proposed to concentrate attention only
in the two-input tables and to consider the series/row of the
considerations which can be drawn for simplification in their
constructions/designs and improvement in the characteristics.

Let us consider the realization of the operation of the
multiplication of digits α_i and β_i by tabular method on simple
basis/base p_i. Let us make table of the numerical values of product
$\alpha_i\beta_i \pmod{p_i}$, where numerical values α_i will be deposited/postponed
along the horizontal, and the numerical values of second cofactor
β_i - on the vertical line. In the points of intersection we will
indicate values $\alpha_i\beta_i \pmod{p_i}$. Fig. 6.34 gives this table for $p_i = 11$. As
can easily be seen this table is symmetrical relative to left and
right diagonals, and it is also symmetrical relative to vertical
lines and horizontals, which pass between numbers $\frac{p_i-1}{2}$ and $\frac{p_i+1}{2}$.
Actually/really, symmetry relative to left diagonal is determined by
the commutation of operation, symmetry relative to right diagonal is
determined by the fact that

$$(p_i - \alpha_i)(p_i - \beta_i) \equiv \alpha_i\beta_i \pmod{p_i}.$$

Symmetry relative to vertical line and horizontal is determined by

the fact that the sum of symmetrical numbers is multiple p, i.e.

$$\alpha_i \beta_i + \alpha_i (p_i - \beta_i) \equiv 0 \, (\text{mod } p_i).$$
$$\alpha_i \beta_i + (p_i - \alpha_i) \beta_i \equiv 0 \, (\text{mod } p_i).$$

In such a way as to restore/reduce table, sufficient to have an information only about its eighth part. Hence appears the real possibility to shorten the table, which realizes the operation of multiplication.

For the solution of the problem indicated it is considered by advisable to use the special coding of numbers α_i and β_i - the so-called "code of tabular multiplication".

Page 332.

Values α_i, lying in the range $\left[0, \frac{p_i-1}{2}\right)$, can be coded by arbitrary method. Values α_i, lying in the range $\left\lfloor \frac{p_i+1}{2}, p_i - 1\right)$, are coded as $p_i - \alpha_i$.

For a difference in the ranges is built-in index γ_α, which is determined as follows:

$$\gamma_\alpha = \begin{cases} 0, \text{если} \ 0 \leqslant \alpha_i \leqslant \frac{p_i - 1}{2}, \\ 1, \text{если} \ \frac{p_i + 1}{2} \leqslant \alpha_i < p_i. \end{cases}$$

Key: (1). if.

Thus, if is preset number α_i, then for obtaining the value $p_i - \alpha_i$ it suffices to invert index γ_α.

Theorem 6.6. If two numbers A and B are preset on basis/base p_i in the code of tabular multiplication $A_i = (\gamma_\alpha, \alpha_i), B_i = (\gamma_\beta, \beta_i)$, then in order to obtain the product of these numbers on modulus/module p_i, it suffices to obtain product $\alpha_i \beta_i \pmod{p_i}$ in the code of tabular multiplication and to invert its index γ if γ_α is excellent from γ_β, i.e.

$$A_i B_i \pmod{p_i} \equiv (\gamma_i, \ \alpha_i \beta_i \pmod{p_i}), \qquad (6.19)$$

where

$$\gamma_i = \begin{cases} \bar{\gamma}, \ \text{если} \ \gamma_\alpha \neq \gamma_\beta, \\ \gamma, \ \text{если} \ \gamma_\alpha = \gamma_\beta. \end{cases} \qquad (6.20)$$

Key: (1). if.

Proof. Let us consider all possible combinations of the relationships/ratios between γ_α and γ_β:

(1)если $\gamma_\alpha = \gamma_\beta = 0,$ (2)то $A_i B_i \pmod{p_i} \equiv \alpha_i \beta_i \pmod{p_i};$
(2)если $\gamma_\alpha = \gamma_\beta = 1,$ (2)то $A_i B_i \pmod{p_i} \equiv (p_i - \alpha_i)(p_i - \beta_i) \times$
$\times \pmod{p_i} \equiv \alpha_i \beta_i \pmod{p_i};$

Key: (1). if. (2). then.

If $\gamma_\alpha = 1,$ while $\gamma_\beta = 0$ or $\gamma_\alpha = 0,$ while $\gamma_\beta = 1,$ that one and the same in view of the commutation of multiplication, then

$$A_i B_i \pmod{p_i} = \alpha_i (p_i - \beta_i) \pmod{p_i} \equiv (p_i - \alpha_i) \beta_i \pmod{p_i} \equiv$$
$$\equiv p_i - \alpha_i \beta_i \pmod{p_i},$$

i.e. is necessary the inversion of the index of product $\alpha_i \beta_i \pmod{p_i}$. On

the basis of the theorem of table given above, that realizes the operation of multiplication, can be structurally/constructionally reduced four times. If we additionally take into account the commutation of the operation of multiplication, then during the preliminary determination of larger of the cofactors table can be reduced two more times.

Page 333.

As the illustration let us consider the layout of the table, which realizes the execution of the operation of multiplication on basis/base p=11. The numerical table of product $\alpha_i \beta_i \pmod{11}$ is given in Fig. 6.34. The vertical and horizontal axes of symmetry are arranged/located between $\frac{p_i-1}{2}=5$ and $\frac{p_i+1}{2}=6$. Let us write out all values of the code of tabular multiplication for p=11. Code α_i, as it is said above, can be selected with any method. Of it it is required only so that it would mutually unambiguously correspond to this digit of basis/base. For simplicity let us take binary positional the code.

	α_i									
	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

(β_i is the row label)

Fig. 6.34. Table of the numerical values of product $\alpha_i \beta_i$ (mod 11)

Page 334.

(1) Цифра	γ	α_i			(1) Цифра	γ	α_i		
1	0	0	0	1	6	1	1	0	1
2	0	0	1	0	7	1	1	1	0
3	0	0	1	1	8	1	0	1	1
4	0	1	0	0	9	1	0	1	0
5	0	1	0	1	10	1	0	0	1

Key: (1). Digit.

Value 0 and $p_i = 11$ we do not code, since multiplication by these
values gives zero, and in this case operation will be performed more
rapid by the simple analysis of operands. If necessary these values
can be also connected with the table.

Let us show now based on examples that with the use of the code
of tabular multiplication for the operands, undertaken from the
different squares of numerical table, always result we will obtain in
the left square which must be virtually realized.

Example. Let us multiply digits $\alpha=3$ $\beta=4$, i.e.

$$\alpha\beta \pmod{11} = (0,011) \cdot (0,100) \pmod{11} =$$
$$= (0,001) \pmod{11} = (0,001).$$

Here were multiplied digits with the zero indices. To result is
assigned zero index.

Example. Digit $\alpha=8$ to multiply by the digit $\beta=3$:

$$\alpha\beta \pmod{11} = (1, 001) \cdot (0, 011) \pmod{11} = (1, 010).$$

Since in the operation participated the digits with the different
indices that the index of result it must be inverted, i.e.

$$\alpha\beta \pmod{11} = (0, 010).$$

Actually/really,

$$\alpha\beta = 8 \cdot 3 \pmod{11} = 2 \pmod{11}.$$

Example. To multiply digit $\alpha=7$ by the digit $\beta=10$:

$$\alpha\beta \,(\text{mod } 11) = (1, 100)\cdot(1, 001)\,(\text{mod } 11) = (0, 100).$$

In the operation participated the digits with the identical indices, that means result does not require correction.

Let us consider the now tabular realization of the operation of addition and let us determine the form of the code, most convenient for both operations.

During the tabular realization of the operation of addition us it can interest the circumstance that for determining the value of the digit of sum is not required the knowledge of the digits of operands separately. Both the step-by-step addition and transfer they are determined by the collective state of the digits of the operands, which have identical number.

Page 335.

In this case for the step-by-step addition it is important to know, identical they or different ones, for forming the transfer are important to know, are both digits single, for the propagation of transfer it is important to know, are these digits different. Thus, the table of addition can be noticeably abbreviated/reduced, if to its input will be given not the n-bit binary operands, but the

certain n-bit code - the so-called "code of the tabular addition",
each of digits of which can have three values: one of them k_{i0}
occurs, if both i-th digits of operands zero; k_{i1}, if they single, and
k_{ip}, if the corresponding digits of operands are different.

If the i digits of the operands of addition are designated
through α_i and β_i, then, obviously,

$$\left. \begin{array}{l} k_{i0} = \bar{\alpha}_i \wedge \bar{\beta}_i, \\ k_{i1} = \alpha_i \wedge \beta_i, \\ k_{ip} = \alpha_i \wedge \bar{\beta}_i \vee \bar{\alpha}_i \wedge \beta_i. \end{array} \right\} \qquad (6.21)$$

The increase in number of sets of table is determined by the
fact that it is now necessary to realize not 2^{2n}, while 3^n
assemblies.

Further simplification in the table is possible, if we use not
only values k_{i0}, k_{i1}, k_{ip}, but also their inverse values. In this case is
obtained sufficiently idle time the logical description of table.
Thus, for instance, Fig. 6.35 depicts the logical description of the
table, which realizes the execution of the operation of addition on
modulus/module $p_i = 29$.

In the logical description of table for the brevity instead of
designations k_{i0}, k_{i1}, k_{ip} are accepted designations k_0, k_1, k_p with
the indication of their inverse values $\bar{k}_0$, $\bar{k}_1$, $\bar{k}_p$. Through-lines in the
separate cages/cells of table indicate the independence of result

from the values of the corresponding digits of operands. By index a
the markedly collective value of the low-order (first) digits of
operands, indices b, c, d, e designate the collective values
respectively of the second, third, fourth and fifth digits of
operands. All assemblies, which relate to one digit of result, are
joined at the output/yield by CF gate.

Let us recall that for the addition on the modulus/module
indicated in general it is required 2^{2n} the assemblies, where n=5,
i.e., $N=2^{10}=1024$ to assemblies. In Fig. 6.35 is described the table,
which realizes the same operation only 108 by assemblies.

Page 336.

1 разряд результата					2 разряд результата					3 разряд результата					4 разряд результата					5 разряд результата				
e	d	c	b	a	e	d	c	b	a	e	d	c	b	a	e	d	c	b	a	e	d	c	b	a
k_0	$\bar{k}_1$	—	—	k_p	k_0	—	—	k_p	$\bar{k}_1$	k_0	—	k_p	k_0	—	k_0	k_0	k_1	—	—	$\bar{k}_p$	k_1	$\bar{k}_1$	—	—
k_0	—	$\bar{k}_1$	$\bar{k}_1$	k_p	k_0	$\bar{k}_1$	—	$\bar{k}_p$	k_1	k_0	—	k_p	k_p	$\bar{k}_1$	—	k_0	k_p	k_1	—	$\bar{k}_0$	k_1	k_1	$\bar{k}_1$	—
k_0	k_1	—	$\bar{k}_1$	k_p	k_0	k_1	$\bar{k}_1$	$\bar{k}_p$	k_1	k_0	—	$\bar{k}_p$	k_p	k_1	—	k_0	k_0	k_p	$\bar{k}_1$	$\bar{k}_p$	k_1	k_1	k_1	k_0
—	k_1	k_1	k_1	k_1	k_0	k_1	k_1	k_0	k_1	k_0	$\bar{k}_1$	$\bar{k}_p$	k_1	—	k_0	k_0	k_0	—	—	$\bar{k}_p$	k_p	k_1	—	—
k_1	—	—	—	k_p	k_1	—	—	k_p	$\bar{k}_0$	k_0	—	k_1	k_1	k_0	k_0	k_0	k_p	k_0	—	k_0	k_p	k_p	k_1	—
k_p	k_0	$\bar{k}_1$	—	k_p	k_1	—	—	k_p	k_0	k_1	—	$\bar{k}_p$	k_p	—	k_0	k_1	k_p	k_p	$\bar{k}_1$	k_0	k_p	k_p	k_p	k_1
k_p	k_0	—	$\bar{k}_1$	k_p	k_p	k_0	—	k_p	$\bar{k}_1$	k_1	—	$\bar{k}_p$	k_0	$\bar{k}_0$	—	k_1	k_1	$\bar{k}_1$	—	k_1	k_p	k_p	$\bar{k}_0$	—
k_p	—	k_1	k_1	k_1	k_p	k_0	$\bar{k}_1$	k_p	k_1	k_1	—	$\bar{k}_p$	k_0	k_0	—	k_1	k_1	—	k_0	k_1	k_p	k_p	k_0	$\bar{k}_0$
k_p	k_1	—	—	$\bar{k}_p$	k_p	k_0	—	k_0	k_1	k_1	—	k_p	k_0	k_0	—	k_1	k_p	k_1	—	k_1	k_0	k_1	k_1	$\bar{k}_0$
k_p	k_p	k_1	$\bar{k}_1$	$\bar{k}_p$	k_p	k_1	—	k_p	$\bar{k}_0$	k_1	—	k_p	k_1	$\bar{k}_0$	—	k_1	k_p	k_p	$\bar{k}_1$	k_1	k_p	k_0	k_1	$\bar{k}_0$
k_p	k_p	k_0	$\bar{k}_0$	k_p	k_p	k_1	—	k_p	k_0	k_p	k_0	$\bar{k}_p$	k_p	k_1	k_1	k_0	k_0	k_1	$\bar{k}_0$	k_p	k_0	$\bar{k}_1$	—
k_p	k_p	k_0	k_0	$\bar{k}_p$	k_p	k_p	k_0	k_p	$\bar{k}_1$	k_p	k_0	k_1	k_1	—	k_1	k_0	k_p	k_0	—	k_p	k_0	—	$\bar{k}_1$	—
k_p	k_p	k_0	$\bar{k}_1$	k_p	k_p	k_p	k_0	k_0	k_1	k_p	k_0	k_1	k_1	k_0	k_1	k_0	k_0	k_0	$\bar{k}_0$	k_p	k_0	—	$\bar{k}_1$	k_0
k_p	k_p	k_0	k_1	k_1	k_p	k_p	$\bar{k}_0$	k_p	$\bar{k}_0$	k_p	k_0	k_p	k_0	—	—	k_0	k_1	$\bar{k}_1$	—	k_p	k_p	k_0	$\bar{k}_1$	—
					k_p	k_p	k_p	$\bar{k}_1$	k_0	k_p	k_0	k_p	k_p	$\bar{k}_1$	k_0	k_0	k_1	k_1	k_0	k_p	k_p	k_p	k_0	k_0
					k_p	k_p	k_1	k_p	k_0	k_p	k_1	$\bar{k}_p$	k_0	k_0	$\bar{k}_0$	k_1	k_p	k_0	—					
										k_p	k_1	$\bar{k}_p$	k_p	—	$\bar{k}_0$	k_1	k_p	k_0	$\bar{k}_0$					
										k_p	k_1	$\bar{k}_p$	k_1	k_0	$\bar{k}_0$	k_p	k_0	$\bar{k}_1$	—					
										k_p	k_1	k_p	k_0	k_0	$\bar{k}_0$	k_p	k_0	k_1	k_0					
										k_p	k_1	k_p	k_1	k_0	$\bar{k}_0$	k_p	k_p	k_0	k_0					
										k_p	k_p	$\bar{k}_p$	k_1	k_0	k_p	k_p	k_1	k_1	$\bar{k}_0$					
										k_p	k_p	k_p	k_0	$\bar{k}_0$	k_p	k_1	k_0	k_1	$\bar{k}_0$					
										k_p	k_p	k_p	k_1	$\bar{k}_0$										
										k_p	k_p	k_1	k_0	$\bar{k}_0$										
										k_p	k_p	k_1	k_p	$\bar{k}_1$										

Fig. 6.35. Logical description of table of addition on modulus/module 29.

Key: (1). ... digit of result.

Page 337.

It must be noted that the code of tabular multiplication is not in principle suitable for the use in the operation of addition, since

one of the bits of this code is symbol γ.

Let us look, how it is necessary to convert this code so that it could be used and as under tabular addition. To value $\frac{p_i-1}{2}$ the code monotonically increases, each step/pitch varying per unit. The symbol γ of it is equal to zero. Beginning from value $\frac{p_i-1}{2}$ to p_i-1, in the code appears the symbol $\gamma=1$, and the value of the code begins to decrease. If we in the presence of symbol $\gamma=1$ will invert the working part of the code in order to ensure his build-up/growth in the value, then for using the obtained code as the code of tabular addition it is necessary to determine the weight of digit γ. The latter is produced simply.

If we through g_γ define the weight of digit γ and to assume that the working part of the code is preserved on $(n-1)$-bit register, then the inverse value of the code of number $\frac{p_i-1}{2}$ will be defined as

$$2^{n-1}-1-\frac{p_i-1}{2}.$$

and weight value it must satisfy following relationship:

$$g_\gamma+2^{n-1}-1-\frac{p_i-1}{2}=\frac{p_i+1}{2},$$

whence

$$g_\gamma=p_i+1-2^{n-1}.$$

Thus can be obtained the code general-purpose both for the tabular multiplication and for the tabular addition.

It is necessary to again note that on the strength of the fact that the operations in the tabular arithmetic are realized simply by the sample of the value of result in terms of the values of input values, but directly arithmetic operations it is not produced, in the tables there can be suitable almost any coding. Special coding has by its target only reduction of the sizes/dimensions of tables.

In general construction/design and fundamental characteristics of tables are determined by the range of input values.

Page 338.

In connection with this is not excluded the possibility of transition in the process of executing the operation to smaller rice or to the work of arithmetic unit directly in the higher step/stage of the system of residual classes. Let be given numeration system with bases/bases $p_1, p_2, \ldots, p_n$ and range $\mathscr{P}$, in which number A is represented in the form $A = (a_1, a_2, \ldots, a_n)$. Digit a_i on basis/base p_i $(i = 1, 2, \ldots, n)$ let us present in the second step/stage of system, i.e., let us select the new system of the bases/bases

$$q_1, q_2, \ldots, q_{k_1},$$

with the range

$$Q_i = \prod_{j=1}^{k_i} q_j,$$

which would ensure at least the nonappearance of the result of any

computer operation above digit α_i for the range. It is obvious that, that as the greatest result of adding two remainders/residues on modulus/module p_i cannot exceed values $2p_i - 2$, we they must have

$$Q_i > 2p_i - 2;$$

since a product of two remainders/residues on modulus/module p_i it cannot exceed $(p_i - 1)^2$, then

$$Q_i \geqslant (p_i - 1)^2.$$

It is logical that the bases/bases of the second step/stage must satisfy the condition

$$q_j < p_i,$$
$$j = 1, 2, \ldots, k_i, \ i = 1, 2, \ldots, n.$$

In the case of applying the second step/stage of bases/bases is considered by advisable initial numbers by program of the translation/conversion to represent immediately in the second step/stage, arithmetic unit to construct without the straight/direct and reverse decoders as the device/equipment, which works only in the second step/stage. And only the final results of calculations should be program translated through first stage to the decimal representation for the final output from the computer. During this construction the fundamental characteristics of tables noticeably will be improved.

Actually/really, a number of assemblies of each table decreases by value

$$\Delta N = p_i^2 - \sum_{j=1}^{k_i} q_j^2. \qquad (6.22)$$

Page 339.

Redundancy decreases on

$$\Delta J = p_i(p_i-1) - \sum_{j=1}^{k_i} q_j(q_j-1) = \Delta N - p_i + \sum_{j=1}^{k_i} q_j. \quad (6.23)$$

The coefficient of the use of table in the second step/stage θ once is more than in the first, where θ is defined as

$$\Theta = \frac{p_i \sum_{j=1}^{k_i} q_j}{\sum_{j=1}^{k_i} q_j^2}. \quad (6.24)$$

In this case, undoubtedly, will be increased the general/common/total discharge/digital configuration of a number during its storage on the binary register, since increases the total number of bases/bases, which do not coincide with the modulus/module of binary register.

Let us consider based on example, as vary tabular characteristics upon transfer to the second step/stage of bases/bases for the operation of addition. Examination let us conduct, not using consideration about simplification in the construction/design, since they are not connected with the value of basis/base.

Example. Let be preset in first stage basis/base p=50. A quantity of assemblies will be defined as $N=50^2=2500$. Let us select the following bases/bases of the second step/stage:

$$q_1=3, \quad \dot{q}_2=5, \quad q_3=7.$$

Here Q= 3•5•7=105>2p.

From (6.22) it follows that in this case a number of assemblies
of table decreases by value

$$\Delta N = 2500 - (9 + 25 + 49) = 2417.$$

Redundancy cr. (6.23) decreases by value

$$\Delta \mathcal{J} = 2417 - 50 + 15 = 2382$$

relative to $\mathcal{J} = 2450$, and the coefficient of use in (6.24) will be
improved θ once where

$$\theta = \frac{50 \cdot 15}{83} \approx 9,$$

i.e. almost by an order.

The digits of the second step/stage of bases/bases can be, in
turn, they are represented in the third step/stage. For example,
digit a_j on basis/base q_j can be represented in the system with
bases/bases $\rho_1, \rho_2, \ldots, \rho_t$ with range $R = \prod_{i=1}^{t} \rho_i$, that satisfies the same
requirements with respect to the second step/stage which satisfied
the second step/stage with respect to the first.

Page 340.

So can be introduced the fourth and higher step/stage. In this case
is ensured the maximum minimization of tables and are improved their
characteristics, but increases the binary discharge/digital

configuration of entire number.

The limitation of an increase in the number of step/stage is the formulated previously condition of the fact that any basis/base of higher step/stage ρ_j must be less than the basis/base of previous step/stage q_i, i.e., $\rho_j < q_i$ for all j and i.

As an example let us consider, in what highest step/stage of bases/bases can be represented the greatest number on the two-digit basis/base.

Example. To find the highest step/stage of bases/bases for executing the operation of addition with base of first stage p=19. One of the possible versions of the second step/stage it can be

$$q_1 = 2, \quad q_2 = 3, \quad q_3 = 5, \quad q_4 = 7.$$

The range of system Q=2•3•5•7=210, i.e., is satisfied the condition

$$Q > 2p_i - 2.$$

Thus, already in the second step/stage we pass to the bases/bases maximum from which $q_4 = 7$. In this case a number of assemblies in the second step/stage will be defined as $N = 2^2 + 3^2 + 5^2 + 7^2 = 87$, and redundancy $y^{(2)}$ - as

$$y^{(2)} = 87 - 17 = 70.$$

Transition to the third step/stage, without having affected basis/base q_1, q_2, q_3, will make it possible to express the maximum

basis/base $q_4 = 7$ in the system of the bases/bases

$$\rho_1^{(4)} = 3, \qquad \rho_2^{(4)} = 5$$

with range R=15, in this case, as can easily be seen, is satisfied the condition

$$R > 2q_4 - 2.$$

Thus, in the third step/stage we work with the bases/bases:

$$\rho_1^{(1)} = 2, \quad \rho_2^{(2)} = 3, \quad \rho_3^{(3)} = 5, \quad \rho_4^{(4)} = 3; \quad \rho_5^{(4)} = 5,$$

in which superscript indicates the equipment with the corresponding basis/base of the previous step/stage. Transition to the fourth step/stage is impossible. The total number of assemblies in the latter/last system will be defined as

$$N_\rho = 2^2 + 3^2 + 5^2 + 3^2 + 5^2 = 72$$

with the redundancy

$$\mathcal{I}_\rho = 72 - 18 = 54.$$

Example. To find the highest step/stage of bases/bases for executing the operation of multiplication with the basis/base of first stage p=99. For one of the possible versions of the second step/stage can be accepted $q_1 = 3$, $q_2 = 5$, $q_3 = 7$, $q_4 = 11$, $q_5 = 13$, with range Q=15015. Since $(p-1)^2 = 9604$, then is satisfied the condition

$$Q > (p-1)^2.$$

Page 341.

For the third step/stage can be selected the following bases/bases

$$\rho_1 = 2; \quad \rho_2 = 3; \quad \rho_3 = 5; \quad \rho_4 = 7,$$

with range R=2•3•5•7=210, since is satisfied the condition

$$R > (q_5 - 1)^2.$$

Thus, in the third step/stage we will obtain the system of the bases/bases

$$\rho_1^{(1)} = 3; \quad \rho_2^{(2)} = 5; \quad \rho_3^{(3)} = 7; \quad \rho_4^{(4)} = 3; \quad \rho_5^{(4)} = 5; \quad \rho_6^{(4)} = 7;$$
$$\rho_7^{(5)} = 2; \quad \rho_8^{(5)} = 3; \quad \rho_9^{(5)} = 5; \quad \rho_{10}^{(5)} = 7.$$

Transition to the fourth step/stage is impossible.

§6.4. Structure of the tables of basic operations.

For constructing the tables of basic operations is represented by most spectacular the use/application of methods of the special coding, which makes it possible to decrease the size/dimension of the tables of addition, subtraction and multiplication four times. The decrease of tables by a factor of eight is less efficient from the point of view of obtaining maximum high speed, since in this case before the input into the table it is necessary to analyze, which of the operands is more, and to respectively place them on the input registers.

From the point of view of the prize of equipment this method also is not so/such effective, as it seems, since the decrease of table two times necessitates the having of a diagram, which analyzes,

which of the operands is more.

In the implementation of operations by tabular methods in a number of cases the further possible decrease of equipment because is constructed not single table, which realizes result in the binary code, but n finer/smaller tables, which realize responses/answers on each of the n digits of the result where n - discharge/digital configuration of register, necessary for storing the digit on the basis/base in question.

In this case fairly often occurs the unification of tables, i.e., the decrease of a quantity of different types of tables, necessary for the realization of arithmetic unit.

As the illustration let us consider the method of the construction of discharging tables for executing the operation of multiplication on basis/base $p=17$ during the use of the code of multiplication.

For simplicity let us consider the case when the values of operands are preset in single-digit code.

The code of multiplication with $p=17$ takes the form

(1) Цифра	(2) Символ	(3) Код	(1) Цифра	(2) Символ	(3) Код
1	0	0001	9	1	1000
2	0	0010	10	1	0111
3	0	0011	11	1	0110
4	0	0100	12	1	0101
5	0	0101	13	1	0100
6	0	0110	14	1	0011
7	0	0111	15	1	0010
8	0	1000	16	1	0001

Key: (1). Digit. (2). Symbol. (3). Code.

Page 342.

For the fulfillment of the operation of multiplication, as is known, necessary to realize one fourth of multiplication table.

Let us write out now the same table for the low-order digit of result, after blackening those squares in which the result has unity on the low-order digit, and after leaving not blackened squares with the zero value of the low-order digit of result (see Fig. 6.36).

Let us construct by analogous method the table of single values for the second digit of the result (see Fig. 6.37). Let us construct the table of the third digit of the result (see Fig. 6.38). and finally let us construct table for the fourth digit of the result (see Fig. 6.39).

Despite the fact that is reduced the size/dimension of each table and is increased their quantity, as a whole occurs the prize in a quantity of equipment, since to the limit is abbreviated/reduced the redundancy of tables and, as we see, are realized only the assemblies of table, corresponding to significant digits of result.

	(1) Первый операнд							
	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	10	12	14	16
3	3	6	9	12	15	1	4	7
4	4	8	12	16	3	7	11	15
5	5	10	15	3	8	13	1	6
6	6	12	1	7	13	2	8	14
7	7	14	4	11	1	8	15	5
8	8	16	7	15	6	14	5	13

(2) Второй операнд

Key: (1). First operand. (2). Second operand.

Page 343.

Fig. 6.36.

Key: (1). First operand. (2). Second operand.

Fig. 6.37.

Key: (1). First operand. (2). Second operand.

Page 344.

Fig. 6.38.

Key: (1). First operand. (2). Second operand.

Fig. 6.39.

Key: (1). First operand. (2). Second operand.

Page 345.

Further decrease of equipment can be achieved/reached because in some tables can prove to be a number of zero values of result less than the number of single values. In this case it is expedient to realize zero values, and result to invert at the output/yield.

The selected by us modulus/module p=17 in the three-low-order digits has an equal quantity of zero and nonzero results. Let us consider under above conditions accepted the realization of step-by-step tables for executing the operation of multiplication on modulus/module p=19. In this case the code of multiplication takes the form:

(1) Цифра	(2) Символ	(3) Код	(1) Цифра	(2) Символ	(3) Код
1	0	0001	10	1	1001
2	0	0010	11	1	1000
3	0	0011	12	1	0111
4	0	0100	13	1	0110
5	0	0101	14	1	0101
6	0	0110	15	1	0100
7	0	0111	16	1	0011
8	0	1000	17	1	0010
9	0	1001	18	1	0001

Key: (1). Digit. (2). Symbol. (3). Code.

The table of results of operation takes the form

(1)Первый операнд

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	10	12	14	16	18
3	3	6	9	12	15	18	2	5	8
4	4	8	12	16	1	5	9	13	17
5	5	10	15	1	6	11	16	2	7
6	6	12	18	5	11	17	4	10	15
7	7	14	2	9	16	4	11	18	6
8	8	16	5	13	2	10	18	7	15
9	9	18	8	17	7	16	6	15	5

(2) Второй операнд

Key: (1). First operand. (2). Second operand.

Page 346.

The table of the single values of the low-order digit of product accepts the form

(1)Первый операнд

(2) Второй операнд

Key: (1). First operand. (2). Second operand.

AD-A098 441   FOREIGN TECHNOLOGY DIV WRIGHT-PATTERSON AFB OH   F/8 9/2
                MACHINE ARITHMETIC IN RESIDUAL CLASSES, (U)
                APR 81   I Y AKUSHSKIY, D I YUDITSKIY
UNCLASSIFIED   FTD-ID(RS)T-0239-81   NL

7 of 8

MICROCOPY RESOLUTION TEST CHART
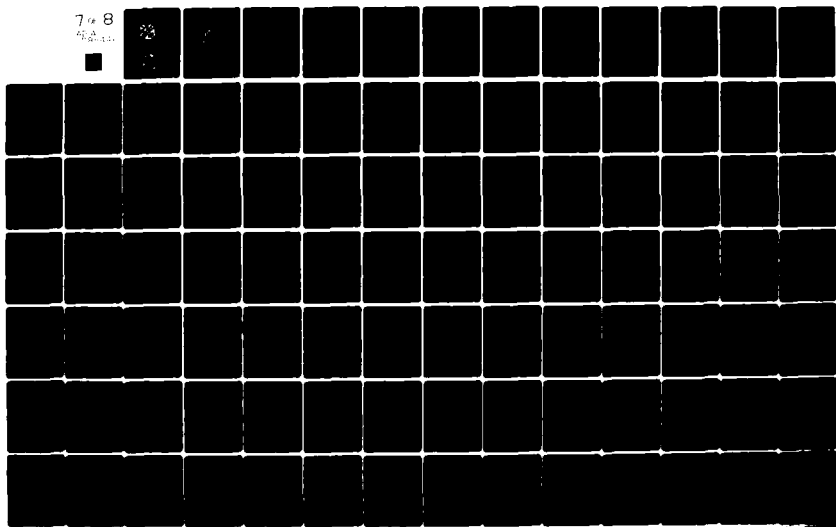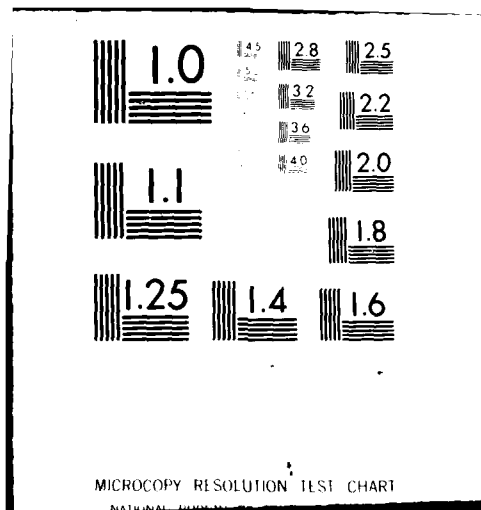
For the second digit of result we obtain

(1) Первый операнд

(2) Второй операнд

Key: (1). First operand. (2). Second operand.

Page 347.

For the third digit of the result

(J) Первый операнд

(J) Второй операнд

Key: (1). First operand. (2). Second operand.

For the high-order code digit of the result we obtain table.

Key: (1). First operand. (2). Second operand.

Page 348.

Here we see that in the table of low-order digit a quantity of zero values of result is noticeably lower than the quantity of single values and it is possible it is more than by 10o/o to decrease the equipment of table, realizing zero values of low-order digit and inverting them at the output/yield of table.

For the second and third digits the picture is reverse. It is here expedient to realize the precisely single values of result.

And finally for the high-order digit are also expedient to realize the single values of result, which compose a total of about 20o/o   table.

Thus, as the most universal method, which makes it possible to substantially decrease the equipment of table, is proposed transition from the direct realization of full/total/complete table to the realization of step-by-step tables taking into account the properties of symmetry. For example, in the implementation of multiplication table on basis/base p=19 for the full/total/complete table it would

be required $19^2=361$ the assemblies, commutated at the output/yield.

In the case of applying the special code of multiplication and step-by-step layout, even without taking into account the decrease of equipment due to the numerical ratio and zero and single values of digits, it is required

$$45 + 36 + 36 + 18 = 135 \quad \text{assemblies.}$$

This calculation is made inaccurately, since, on one hand, was not considered the complexity of the assemblies (in the step-by-step tables they are substantially simpler), and on the other hand, was not considered the circumstance that in the step-by-step tables to the input is fed the single-digit code for forming which is also necessary the corresponding equipment.

In practice during the reasonable engineering of tables additionally to obtain, on the average from 20 to 40o/o of economy of equipment.

Substantially more simply and more economically are realized single-input tables, i.e., the tables, working from one operand at the input, since they are realized with the zero redundancy and they barely require the enlistment of any methods, which simplify their

construction/design.

Page 349.

§6.5. Principles of the construction of basic building blocks of arithmetic unit.

One of the distinctive properties of the system of residual classes is the possibility of the independent and parallel processing of each digit of a number in the majority of the operations of arithmetic unit.

In connection with this in the arithmetic unit can be isolated the series/row of circuits according to a number of bases/bases, which work in the majority of the cases independently of each other and in parallel in the time.

In the operations, which carry positional character, this independence of circuits fails and the result of their work is analyzed together for the determination of the positional characteristics of a number.

But in a whole series of machine operations circuits function independently and independently, defining the time of the execution

of entire operation by the time of its execution in the longest circuit, and they can be designed as standard design.

The standard structural/design formulation of circuits has the further advantage, which consists in simplification in the redundancy of arithmetic unit.

Determination. By the elementary component/link of arithmetic unit is understood the functional subassembly, intended for the execution on the independent foundation of the system of operations, realized independently, and structurally/constructionally designed into the standard circuit of arithmetic unit.

Here by the word "operation" is understood not only the single operation of arithmetic unit, wholly realized by the independent circuits, but also the individual part of such operation, in which is withstood the mentioned independence of circuits.

Let us consider in more detail, which from itself represents the elementary component/link of arithmetic unit.

The block diagram of the elementary component/link of arithmetic unit is represented in Fig. 6.40.

Through Rg is designated the binary register, intended for
storing the binary code of the single digit of a number.

Page 350.

In all is assumed the presence of two registers Rg1 and Rg2, intended
for the storage codes of operands, moreover to the register Rg2 will
be brought in result and from it is produced the readout of
operation.

Through KT is designated the deck of tables. Single table we
will designate by index I_t. Under the table let us agree on
subsequently to understand the functional diagram, intended for
executing of individual operation or single operation on this
basis/base, although structurally/constructionally it can consist of
several parts (for example, when selecting of the step-by-step method
of organizing the tables).

Tables can be realized on any technical basis. For the certainty
we will proceed from the potential mode of their operation. This will
permit us to examine tabular type diagrams, which work directly to
each other, moreover result from the output/yield of terminal table
will be obtained without the further control signals.

Inclusion/connection the top or another table of the deck of tables is produced by the feed to it of control voltage along channel CK - the "symbol of instruction".

Through τ_{0i} we will designate triggering time of table on the greatest basis/base with the execution of the i operation.

Result of operation is preserved on the register Rg2. If triggering time of table is small in comparison with the time of the change-over of input registers, then the straight/direct recording of result of operation on Rg2 is impossible. Therefore between the output/yield of table and the input is connected "delay circuit" (SZ).
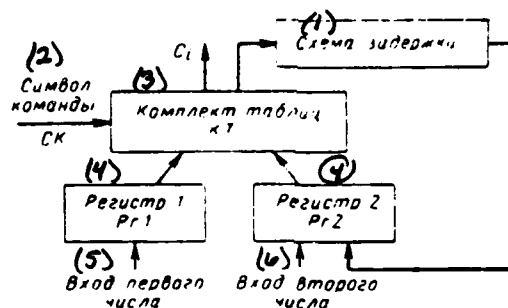
Fig. 6.40. Block diagram of the elementary component/link of arithmetic unit.

Key: (1). Delay circuit is. (2). Symbol of instruction. (3). Deck of tables. (4). Register. (5). Input of first number. (6). Input of second number.

Page 351.

As the delay circuit can be used intermediate register, delay lines or any special diagrams.

The deck of tables has the second output/yield, designated c_i, which is intended for the participation in determining of the positional characteristics of entire number.

If we designate the time of the change-over of the register

through r_1, and delay factor which ensures the delay circuit, through r_2, then total time τ_i of the execution of the i operation on the assumption that the operands are arranged/located on the input registers of elementary component/link, will be defined as

$$\tau_i = \tau_{0i} + \tau_1 + \tau_2,$$

and the read-out time of result on output/yield c_i will be equally to τ_{0i}.

Determination. By the generalized component/link of arithmetic unit or simply component/link we will call the set of elementary components/links on all basis of system.

If in the operations, performed by arithmetic unit, were not included positional type operations, then device/equipment would consist only of component/link and local control unit. The presence of positional type operations determines need in the introduction to the composition of the arithmetic unit of the so-called block of positional characteristics (b.p.kh.).

Determination. The unit of the positional characteristics of arithmetic unit we will call the functional box, intended for determining the minimum trace of a number or, that the same, for numbering of the interval in which is arranged/located a number.

In chapter 5 is examined the series/row of the methods of determining the minimum trace of a number. From consecutive type methods let us select the method of nulling and will consider how will appear the unit of positional characteristics in the implementation of this method.

If is carried out the process of nulling on i digits i=1, 2, ..., n-1 is obtained the number

$$(0, 0. ..., 0, \alpha_{i+1}, \alpha_{i+2}, ..., \alpha_n), \qquad (6.25)$$

then for the following stage of nulling is chosen the constant whose i of the first digits - zero, (i+1) digit coincides with digit $p_{i+1} - \alpha_{i+1}$, the others digits are such that the selected constant would have the smallest possible value.

Page 352.

Then during the addition of number (6.25) with this constant is nulled next i+1 digit and in this case is ensured the nonappearance from the working range.

By distinctive features of this process is change at each step/pitch of the values of the digits greater than the nulled one, i.e., system the sequence of process. Actually/really, without having finished the previous step/pitch completely, i.e., without having

fulfilled to the end the addition in the previous stage, we do not
know the more significant digits of the number according to which at
the subsequent steps/pitches will be determined the constants of
nulling.

Furthermore, with the execution of the process indicated we each
time work with entire number, although a quantity of significant
digits of number and significant digits of constants always is
reduced.
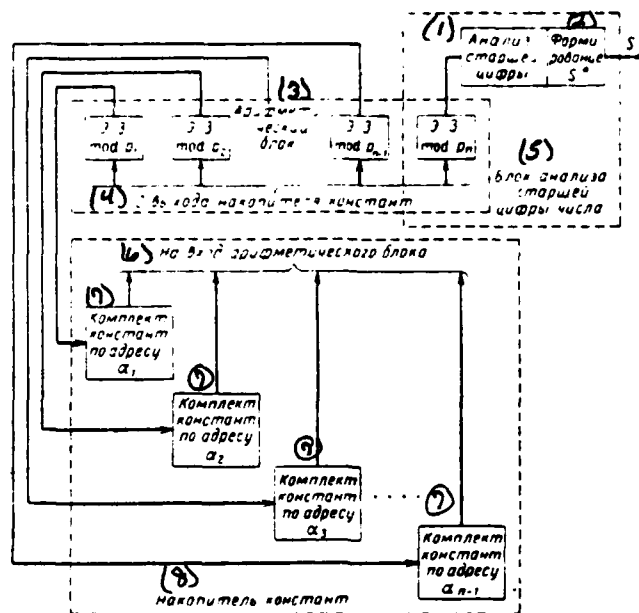
Fig. 6.41. Unit of positional characteristics (version of nulling).

Key: (1). Analysis of more significant digit. (2). Formation. (3).
Arithmetic unit. (4). From output/yield of accumulator/storage of
constants. (5). Unit of analysis of more significant digit of number.
(6). To input of arithmetical unit. (7). Deck of constants with
address. (8). Accumulator/storage of constants.

Page 353.

It is obvious that in the basic building block of positional
characteristics must they consist of the deck of the

devices/equipment of storage of the constants, rotation/access into
each of which is produced the appropriate digit of a number as this
shown in Fig. 6.41, and the unit of the analysis of more significant
digit.

It is logical that the constants, selected in terms of the value
of the digit of basis/base p_1, have significant digits on all
bases/bases, including p_1, the constants, selected in terms of the
value of the digit of basis/base p_2, have to one significant digit
less, and further, passing from one basis/base to the following, we
each time use with the constants, which have to one digit less, and
finally the latter/last group of constants has only two significant
digits. On the other hand, taking into account the ordering of the
system of bases/bases, from one basis/base to the next increases a
quantity of constants which must be preserved. In other words, in the
accumulators/storage in question consistently increases a quantity of
preserved words from p_1-1 to p_n-1 and in this case is reduced the
discharge/digital configuration of these words on (n-1) digit in the
word to one digit.

After designating the access time of constant from the
appropriate accumulator/storage through $\tau_{ами}$, we will obtain time
$\tau_{н1}$ of the execution of the entire operation of the nulling

$$\tau_{н1} = (n-1)(\tau_{ами} + \tau_{ами}).$$

With the execution of the accumulators/storage of constants by
tabular method it is possible to assume that the time of access to
accumulator/storage and the time, necessary for adding two numbers of
one order, $\tau_{вы6} \approx \tau_{выч} = \tau_{сл}$. Then

$$\tau_{нт} \approx 2(n-1)\tau_{сл}.$$

The version of the execution of the operation of nulling
examined is not clearly optimal from the point of view of high speed,
since the execution of addition and the sample of next constant are
spread in the time.

It was assumed that, until is completed addition, to us was not
known the digit on which must be selected the constant for the
following stage of nulling.

However, thus far is produced the sample of constant for the
number

$$(0, 0, \ldots 0, \alpha_i, \alpha_{i+1}, \ldots, \alpha_n)$$

in terms of the value of digit α_i, on basis/base p_i, in the
elementary component/link, which works on basis/base p_{i+1}, it can be
prepared the value of digit α_{i+1}, on which in the following stage
will be produced the sample of constant.

Page 354.

Is actual/real, the value Δa_{i+1}, which will be subtracted from a_{i+1}, in order to obtain a'_{i+1}, it is determined only by value a_i.

Therefore if in the process of the sample of constant in terms of value a_i, the latter will be transmitted into the elementary component/link, which works on basis/base p_{i+1}, then in terms of value a_i and a_{i+1} from the appropriate table can be selected value a'_{i+1}.

But in this case in the constant, selected in terms of the value of digit a_i, there is no need to have a digit on basis/base p_{i+1}, i.e. the discharge/digital configuration of constants decreases by one more digit, which respectively decreases the equipment of the accumulators/storage of constants.

If a previously quantity of the preserved digits S_1 was defined as

$$S_1 = \sum_{i=1}^{n-1} (p_i - 1)(n - 1),$$

then now it will be defined as

$$S_2 = \sum_{i=1}^{n-2} (p_i - 1)(n - i - 1),$$

i.e. it decreases on

$$\Delta S = \sum_{i=1}^{n-1} (p_i - 1).$$

The temporary/time performance record of the unit of nulling in

this case is represented in Fig. 6.42.

For convenience in the description are introduced the following abbreviations:

- rotation/access after the constant in terms of the value of digit a_i let us designate ~~about~~ $Ob\,a_i$;

- formation/education of following digit a_{i+1} in the elementary component/link, which works on modulus/module p_{i+1}, to be designated a_{i+1};

$$\frac{\Sigma_1 \quad \Gamma^{\prime} x_j \quad \Sigma_6 \quad \Sigma_{-6} \quad 06\alpha_7^{\prime} \quad \Sigma_{(m-1)-n} \quad \Sigma_n \quad \Sigma_n}{C6\alpha \quad \Sigma_{\cdot\cdot} \quad \Sigma_j \cdot \quad 2^{\prime}\alpha_j \quad \Sigma_{6-} \quad 06\alpha_{m-3}}$$

$$\alpha_1^{\prime} \; 06\alpha_2^{\prime} \; \alpha_3 \; \alpha_4^{\prime} \; 03\alpha_5^{\prime} \; \alpha_3 \; \alpha_6 \; 06\alpha_4^{\prime} \; \alpha_7^{\prime} \; \alpha_8 \qquad \alpha_{n-2}^{\prime} \; 06\alpha_{n-2}^{\prime} \; \alpha_{n-1}^{\prime}$$

Fig. 6.42. Temporary/time performance record of the unit of nulling.

Page 355.

- the addition of nullized number with the constant, which has significant digits, beginning from the digit on basis/base p_i, we will designate Σ_{i-n}.

A number of additions in the version in question is also equal n-1, since the nulling is conducted through all n-1 digits. However, after every two additions is required one further stroke/cycle for forming of next address and rotation/access into the accumulator/storage. Fig. 6.43 depicts one standard group of the time graph.

With addition Σ_{i-n} simultaneously is produced the rotation/access into accumulator in terms of the value of digit α_{i-1}. It is impossible to combine these operations with the formation/education of address α_i since the elementary component/link, which works on basis/base p_i, is occupied with the operation of addition. In the following stroke/cycle with addition

$\Sigma_{(i+1)-n}$ is combined the formation/education of address a_i. It is impossible to fulfill in following addition time : $\Sigma_{(i+2)-n}$ since is not carried out the sample on digit a_i. In connection with this to every two addition times falls one stroke/cycle, free from the addition.

Thus, the total quantity of strokes/cycles, free from the addition, during which is produced the access to accumulator/storage and the formation/education of next address, will be defined as $[n/2]$, and the total operation time of nulling as

$$\tau_{u2} = (n-1)\,\tau_{cn} + \left[\frac{n-2}{2}\right]\tau_{su6}.$$

Taking into account, as earlier, that

$$\tau_{su6} = \tau_{cn},$$

we will obtain

$$\tau_{u2} = \left(\left[\frac{n-2}{2}\right] + n - i\right)\tau_{cn}.$$

$$
\begin{array}{c|c|c}
\Sigma_{i \cdot n} & \Sigma_{(i+1) \cdot n} & 06\,\alpha'_i \\
\hline
06\,\alpha'_{i-1} & \alpha'_i & \alpha'_{i+1}
\end{array}
$$

Fig. 6.43. Standard group of time graph.

Page 356.

With n even we will obtain.

$$\tau_{H2} = \left(\frac{3}{2}n - 2\right)\tau_{cn},$$

also, with n odd

$$\tau_{H2} = \frac{3n-5}{2}\tau_{cn}.$$

In general with n even we obtain shortening the operation time on

$$\Delta\tau_H = \tau_{H1} - \tau_{H2} = \left(2(n-1) - \frac{3}{2}n + 2\right)\tau_{cn} = \frac{1}{2}n\tau_{cn}$$

or in the percentages

$$\frac{\Delta\tau_H}{\tau_{H1}}\,100\% = \left(25 - \frac{25}{n-1}\right)\%,$$

i.e. not less than to 25o/o.

If n odd, we obtain shortening the operation time on

$$\Delta\tau_H = \frac{n+1}{2}\tau_{cn}$$

or in the percentages

$$\frac{\Delta\tau_H}{\tau_{H1}}\,100\% = \left(25 + \frac{50}{n-1}\right)\%.$$

Is feasible also the version of pair nulling. The set of constants of this case consists of

$$p_1 p_{n-1} - p_2 p_{n-2} - \ldots - p_{\frac{n-1}{2}} p_{\frac{n-1}{2}} -$$

$$-\frac{n-1}{2} = \sum_{i=1}^{\frac{n-1}{2}} (p_i p_{n-i} - 1) \quad \text{(1)} \quad \text{констант или}$$

$$S_3 = \sum_{i=1}^{\frac{n-1}{2}} (p_i p_{n-i} - 1)(n - 2i) \quad \text{(2)} \quad \text{цифр.}$$

Key: (1). constants or. (2). digits.

The process of nulling a number consists of n-1/2 steps/pitches. The block diagram of device/equipment is given in Fig. 6.44.

The total time, necessary for nulling of a number by the method in question, will be defined as

$$\tau_{H3} = \frac{n-1}{2} (\tau_{вшб} - \tau_{сл}).$$

Page 357.

Here already it cannot be assumed that $\tau_{вшб} \approx \tau_{сл}$, since are required the accumulators/storage of the constants of the relatively great capacity which hardly can be realized by tabular methods. However, taking into account that each of of the accumulators in the process nulling works only on the sample of one constant, i.e., with the frequency, in n-1/2 times of less than the frequency of the steps/pitches of nulling, we, drawing the effort of

accumulators/storage, can assume/set

$$\tau_{вмб} \approx \tau_{сл}.$$

Then

$$\tau_{н3} \approx (n-1)\,\tau_{сл}.$$

The time of the execution of nulling by the method indicated is shortened on

$$\Delta\tau_н = \tau_{н1} - \tau_{н3} = (n-1)\,\tau_{сл}$$

or in the percentages

$$\frac{\Delta\tau_н}{\tau_{н1}}\,100\% = 50\%.$$

i.e. process proceeds, as one would expect, two times it is more rapid.

As an example let us consider, how the relationship/ratio of the storage capacity of constants in all three methods of nulling on the assumption that is preset the system of the bases/bases:

$$p_1 = 37, \quad p_2 = 41, \quad p_3 = 43, \quad p_4 = 47, \quad p_5 = 53, \quad p_6 = 59, \quad p_7 = 61.$$
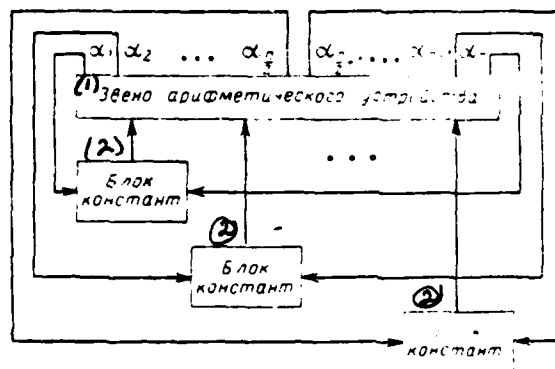
Fig. 6.44. Device/equipment of the pair nulling of a number.

Key: (1). Component/link cf arithmetic unit. (2). Unit of constants.

Page 358.

Digits on all basis of system require for the storage 6-digit binary registers. Since with an increase in the basis/base is reduced a quantity of significant digits, then we will consider total storage capacity in a quantity of digits which must be preserved.

For the first method

$$S_1 = \sum_{i=1}^{6} (p_i - 1)(n - i) =$$
$$= 36 \cdot 6 + 40 \cdot 5 + 42 \cdot 4 + 46 \cdot 3 + 52 \cdot 2 + 58 \cdot 1 = 884 \text{ цифры.} \quad (1)$$

Key: (1). digit.

For the second method

$$S_2 = \sum_{i=1}^{5} (p_i - 1)(n - i - 1) =$$
$$= 36 \cdot 5 + 40 \cdot 4 + 43 \cdot 3 + 46 \cdot 2 + 52 \cdot 1 = 613 \text{ цифр.}^{(1)}$$

Key: (1). digits.

⟵ And finally for the third method

$$S_3 = \sum_{i=1}^{3} (p_i p_{n-i} - 1)(n - 2i) =$$
$$= (37 \cdot 59 - 1) 5 + (41 \cdot 53 - 1) 3 + (43 \cdot 47 - 1) = 19\,446 \text{ цифр.}^{(1)}$$

Key: (1). digit.

The same values can be compared between themselves, after leading to certain standard accumulator/storage, which has word with a length of into 30 digits, although in reality this comparison carries purely conditional character.

Then total capacitance in the first case is conditionally equivalent to accumulator/storage with a capacity/capacitance of into 177 words, in the second case — to accumulator/storage with a capacity/capacitance of into 123 words and in the third case to accumulator/storage with a capacity/capacitance of into 3839 words.

Let us consider now possible realization of one of the parallel methods of determining minimum trace of a number, in particular the method of expanding the range.

In this method, as is known, is assigned number A by digits $\alpha_1, \alpha_2, \ldots, \alpha_n$ and is determined digit α_{n+1}, with which a number it is correct in the expanded range. Moreover, if S_A is trace of number A, then initially is produced the expansion of the number

$$M_A = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, S_A),$$

rank of which is computed from the formula

$$r_{M_A} = \sum_{i=1}^{n-1} r_i - \pi_A m_n,$$

where r_i — rank of the corresponding minimum of pseudo-orthogonal number, and π_A — number of transitions on basis/base p_n with formation/education S_A.

Page 359.

Then digit $\alpha_{n+1}^{(s)}$ of the expanded representation of number M_A is equal to

$$\alpha_{n+1}^{(s)} = (q - r_{M_A}) \pmod{p_{n+1}}.$$

First of all here should be focused attention on the fact that the majority of the values, which participate in the calculation, are only the functions of the digits of an initial number and for the operations with them it is possible to use values α_i (i=1, 2, ..., n-1), recoding them at the input of the corresponding table. Let us

introduce the designation of some recoded values: the value of trace S_i^* of the minimum pseudo-orthogonal number

$$M_i = (0, 0, \ldots, \alpha_i, 0, \ldots, S_i^*)$$

we will designate $S_i^* = f_1(\alpha_i)$, and rank its $r_i = f_2(\alpha_i)$, member of the generalized sum of the digits of number M_A let us designate

$$\lambda_i \alpha_i = f_3(\alpha_i).$$

Here

$$\lambda_n S_A = f_3(S_A).$$

Then the trace of number A can be registered as

$$S_A = \sum_{i=1}^{n-1} f_1(\alpha_i) \, (\mathrm{mod}\, p_n),$$

and digit $\alpha_{n+1}^{(\text{e})}$ - as

$$\alpha_{n+1}^{(\text{e})} = \Big(\sum_{i=1}^{n-1} F(\alpha_i) + f_3(S_A) - \pi_A m_n \Big) \, (\mathrm{mod}\, p_{n+1}),$$

where

$$F(\alpha_i) = (f_3(\alpha_i) - f_2(\alpha_i)) \, (\mathrm{mod}\, p_{n+1}).$$

Through $f_4(\alpha_n)$ let us designate the corrective term for number M_A, the determined by values α_n and S_A, after addition which to number M_A is obtained number A_1, which coincides with number A in digits $\alpha_1, \alpha_2, \ldots, \alpha_n$. In this case is produced the sign/criterion γ, which is determining (with $\gamma = 1$) the presence of critical situation.

Page 360.

DOC = 81023917   PAGE

Then digit $\alpha_{n+1}^{(1)}$ on basis/base p_{n+1} of number A_1 can be defined as

$$\alpha_{n+1}^{(1)} = \left(\sum_{i=1}^{n} F(\alpha_i) + \pi_A m_n \right) (\bmod\, p_n), \qquad (6.26)$$

where

$$F(\alpha_n) = (f_3(S_A) - f_4(\alpha_n)) (\bmod\, p_{n-1}).$$

The realization of expression ((6.26) assumes the presence of three groups of the equipment: the first group of equipment for the error of trace S_A, simultaneously with it π_A and a number of incorrect pairs λ, the second group of equipment for calculation $\sum_{i=1}^{n-1} F(\alpha_i) (\bmod\, p_{n+1})$ and the third group of equipment for final calculation $\alpha_{n+1}^{(1)}$ and analysis of critical situation, if it occurs.

Fig. 6.45 depicts the first group of equipment. It consists of the two-input adders, designated by index Σ with the indication, on what modulus/module they work.
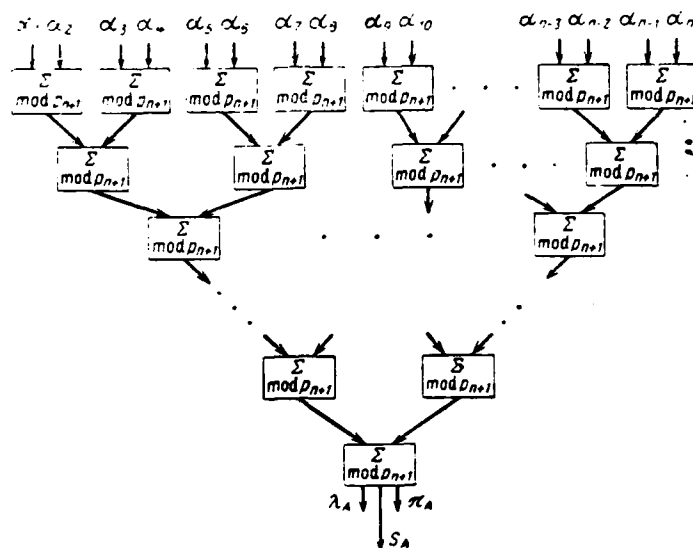
Fig. 6.45. Block diagrams of the calculation of the trace of a number.

Page 361.

In all it will be required by k of the steps/stages of tables, which work to each other where k - smallest positive number, determined from the condition

$$2^{k-1} < n-1 \leqslant 2^k.$$

In this case the computing time S_A and π_1 in general is defined as $k r_0$.

The second group of equipment is performed also on basis k of the steps/stages of tables. Calculation with its help of value $\sum_{i=1}^{n-1} F(\alpha_i) \pmod{p_{n+1}}$ is produced after kr_0 time intervals. A difference in the first two groups of equipment consists only of the coding of values α_i (i=1, 2, ..., n-1) at the input of the tables of first stage.

In the second group of equipment in proportion to the addition of values $\dot{F}(\alpha_i)$ are summarized binary signs/criteria k, being determining the parity of the minimum pseudo-orthogonal numbers each of which is wholly determined by value α_i ((i=1, 2, ..., n-1). Thus, at the output/yield simultaneously with value $\sum_{i=1}^{n-1} F(\alpha_i) \pmod{p_{n+1}}$ is computed the value of the parity of number M_A, namely:

$$\psi(M_A) = \sum_{i=1}^{n-1} k_i \pmod 2.$$

And finally the third group of equipment, represented in Fig. 6.46, realizes calculation $\alpha_{n+1}^{(i)}$ and sign/criterion γ. If the critical case does not take place ($\gamma=0$), then value $\alpha_{n+1}^{(i)}$ is the unknown minimum trace of a number. But if the critical case takes place ($\gamma=1$) then it is necessary to analyze the relationship/ratio of parities $\psi(A_1)$ and $\psi(A_B)$. Parity $\psi(A_1)$ is determined by simple summation over the binary modulus/module of the values of parities $\psi(M_A)$ of number M_A and parity $\psi(f_+(\alpha_n))$ of corrective term

$\psi(A_1) = (\psi(M_A) - \psi(f_+(\alpha_n))) \pmod 2.$ In terms of value $\psi(A_1)$ and α_{n+1} can be

determined value N' and, if occurs situation $N' < \frac{p_{n+1}-1}{2}$ or

$N' \geqslant \frac{p_{n+1}-1}{2}$, when value $\psi(A_\beta)$ it is immediately determined, at the

output/yield γ_2 appears the indication, which of the values α_{n+1} or

β_{n+1} is unknown.

Page 362.

If occurs situation $N' = \frac{p_{n+1}-1}{2}$,   then is produced sign/criterion γ_3,

and then indication about validity α_{n+1} or β_{n+1} is removed/taken from

the output/yield γ_4.

Fig. 6.47 depicts the block diagram of the full/total/complete

unit of positional characteristics for the parallel version. The

total time τ_1 of the definition of the minimum trace of a number in

the noncritical case will be defined as

$$\tau_1 = (k+2)\tau_0, \qquad (6.27)$$

and in the critical case

$$\tau_2 = (k+3)\tau_0. \qquad (6.28)$$

Here

$$\log_2(n-1)+1 > k \geqslant \log_2(n-1).$$

Total quantity N_τ of tables there will be the order

$$N_\tau \approx 2(2^k-1)+5 = 2^{k+1}+3, \qquad (6.29)$$

since a quantity of tables during their organization in k of

steps/stages is equal to $2^k - 1$.
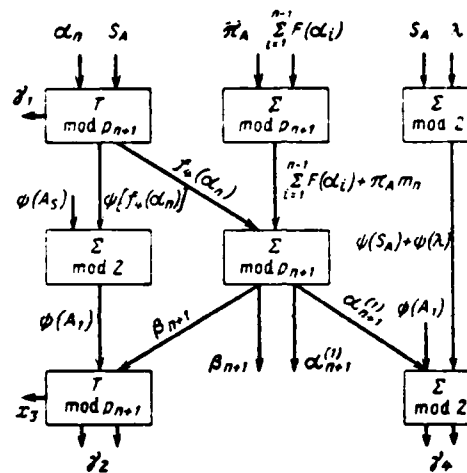
Fig. 6.46. Third group of the equipment of the unit of the positional characteristics of a number.

Page 363.

As the illustration Fig. 6.48 gives the block diagram of the unit of positional characteristics for the case of ten bases/bases

$$n + 1 = 10.$$

Here k=3, whence $r_1 = 5r_0$, $r_2 = 6r_0$ and $N_T = 19$;   as this follows from (6.27), (6.28) and (6.29).

The unit of positional characteristics, computing the value of the minimum trace of a number, simultaneously serves the purposes of the checking of the correctness of a number, since by the simple

comparison of value S* with the value of the digit of a number on

basis/base p_{n+1} we determine its correctness, in other words, the

presence or the absence cf the error in a number.

In general into the structure of the arithmetic unit, which

works on bases/bases $p_1, p_2, \ldots, p_n, p_{n+1}$, where basis/base p_{n+1} is

control room, must enter two similar units; they of them, the

defining minimum trace according to basis/base p_{n+1} is the unit of

check to the presence of the error in a number, and the second, that

defines the value of minimum trace according to basis/base p_n is

strictly the unit of positional characteristics, which defines the

location of entire number in the numerical range and which realizes

the operations of positional character, such, as the determination of

the sign of a number, arithmetic comparison, etc.
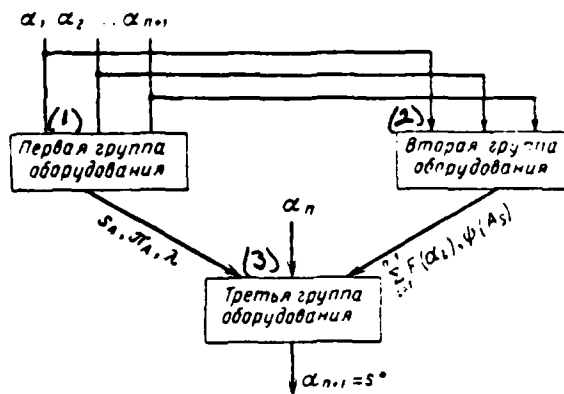
Fig. 6.47. Unit of the positional characteristics of a number.

Key: (1). First group of equipment. (2). Second group of equipment.
(3). Third group of equipment.
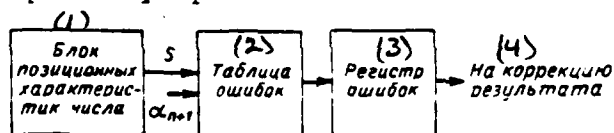
Fig. 6.48. Unit of check.

Key: (1). Unit of the positional characteristics of a number. (2).
Table of errors. (3). Register of errors. (4). For correction of
result.

Page 364.

In the unit of check additionally to the equipment of the unit
of positional characteristics is connected the table of the selection

of the alternative sets of errors and register for their storage as
this is shown in Fig. 6.48. In proportion to the contraction of
alternative set from the contained register are excluded the errors,
which cannot occur, but after the end of process in terms of the
value of error is produced the correction of result.

§6.6. On the structure of digital computers in the system of residual
classes.

Questions of the structure of digital computers are extremely
vast and by themselves are the object/subject of wide and in-depth
experiments. Is known a whole series of the publications, dedicated
to fundamental research of the bases of theory and practice of
designing the digital computers of the most diverse
designation/purpose.

The being investigated in the present monograph system of
residual classes is the very peculiar numeration system and as any
numeration system, are set limitations not on the structure of entire
machine as a whole, but only to the structure of arithmetic unit in
light of the peculiar treatment of the algorithms of the series/row
of the operations of arithmetic unit.

In this plan/layout the conducting research of the structures of

computers and selection of the optimum versions of the organization
of entire machine are fully applicable also to the machines,
constructed in numeration system in question. Even the arithmetic
unit, most dependent on the adopted system of numeration, can be
organized on the basis of the concepts, accepted in arithmetic
devices of positional machines.

However, on the other hand, the system of residual classes
possesses, as we were convinced, the next very specific properties,
which do not have analog in the positional numeration systems.

Page 365.

Because of this specific character it was possible to construct the
so-called tabular arithmetic, not applied in the positional machines,
to work out the new principles of detection and correction of errors,
and on the basis their arithmetic of errors, that also is impossible
in the case of the positional system of numeration, etc.

Therefore by very advisable ones is considered further
development of research in the region of the structure of machines,
directed toward the maximum utilization of the specific character of
nonpositional systems for the purpose of an essential improvement in
the structural parameters of digital computers, especially this

parameter as flexibility. In this connection it is possible to divide
all the equipment of digital computer into two groups:

The first group - equipment, connected with the representation
of a number according to the independent foundations. Here can be
referred the elementary components/links of arithmetic unit, all
forms and the step/stage of the accumulators/storage of numbers,
entire system of index registers, introduction system - output of
information.

Note. It is assumed that the system of index registers is
carried out in the nonpositional version.

Actually/really, the addressing of accumulators/storage it is
expedient to fulfill also in the residual classes, since already in
the accumulators/storage of average/mean capacity/capacitance the
modified part of the address is congruent in a quantity of digits
with the mantissa of a number. Hence the rates of the arithmetic
processing of a number and address must be congruent, since otherwise
can be broken the balance between the efficiency of the arithmetic
and memory unit.

Second group - equipment, connected with the operations on
entire number and with the organization of the work of all

devices/equipment of machine. Here are involved the unit of
positional characteristics and the unit of check, the overwhelming
majority of the control system, the accumulator/storage of
instructions, etc. During this division it is possible to claim that
the first group, which consists, in essence, from the mass channels,
and therefore, that encompasses the suppressing capacity of TsVM
[digital computer] on the basis of the traced in chapter 4
acquisition systems and correction of errors can be made maximally
tenacious without a noticeable increase in the equipment. This means
that the appearing failure is corrected, and with an increase in the
number of failures machine continues correctly to function, but in
the smaller numerical range, i.e., with the smaller accuracy.

Page 366.

The second group of equipment, which comprises, on our calculations, about 20-30c/o of entire equipment, must be defended by the known methods of redundancy.

In the structural/design plan/layout of very promising is represented the idea of the organization of the first group of equipment in the form of single machines of circuits.

Under machine circuit is understood the equipment of the mass channels of the introduction system - output, of accumulators/storage of numbers of all forms and steps/stages and the elementary component/link of arithmetic unit, which works on the independent foundation.

If we compose each machine circuit with its local control, then noticeably grows the percentage of functionally tenacious equipment.

Further, in the system of residual classes is very uniquely solved the problem of automatic equipment scaling by the introduction

of the floating range. In all devices/equipment of computer, except arithmetic unit, numbers can be represented in the range $[0, \mathscr{P})$ on bases/bases $p_1, p_2, \ldots, p_n$.

In the arithmetic unit the range of the representation of numbers $[0, P)$ can be substantially increased due to the introduction of the series/row of additional bases/bases $p_{n+1}, p_{n+2}, \ldots, p_{n+m}$:

$$P = \mathscr{P} \prod_{i=1}^{m} p_{n+i}.$$

Assuming/setting the mantissas of operands by those represented in the range $[0, \mathscr{P})$, unavoidably we come to the fact that the results of arithmetic operations can lie/rest at the broader band. In particular, for the representation of the result of operation of multiplication we should to have a range of the order $[0, \mathscr{P}^2)$, and this means that after the admission into the arithmetic unit the mantissas of operands must be represented in the broader band $[0, P)$, where $P > \mathscr{P}^2$. Then the result of arithmetic operation is exact, but it it is necessary to reduce to the form, which makes it possible to transport it into other devices/equipment of machine, which use in the range $[0, \mathscr{P})$, for which it is necessary to produce rounding on the additionally introduced bases/bases.

As is known, rounding on basis/base p_j consists in the reduction of a number to the form, which separates on p_j, i.e. in the subtraction from entire number of digit on this basis/base and in the

division of the obtained result on p_j.

Page 367.

On the strength of the fact that all basis of the expanded system are mutually prime numbers, but after division on p_j is light on this basis/base no longer interests, the indefinite situations of form 0/0 arise cannot.

Let the result of arithmetic operation take the form
$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}, \ldots, \alpha_{n+m}).$$
then after the turning of range we obtain
$$A \approx p_{n+1}^{\delta_1} p_{n+2}^{\delta_2} \cdots p_{n+m}^{\delta_m} (\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_n). \quad (6.30)$$
where $\delta_j (j = 1, 2, \ldots, m)$ is the binary function, which takes the values p_j.

$\delta_j = 1$, if was produced rounding on basis/base

$\delta_j = 0$, if roundings was not produced.

Determination. Under the natural form of the representation of a number in the residual classes we will understand representation of the form (6.30), in which the mantissa of a number is arranged/located in the range $[0, \mathscr{P})$.

Determination. The turning of range we will call the process of transition from the representation of mantissa in the range [0, P) to its representation in the range [0, $\mathcal{P}$).

Expression (6.30) leads us to the following representation of entire number

$$A = p_{n+1}^{\widetilde{g_1}} p_{n+2}^{\widetilde{g_2}} \cdots p_{n+m}^{\widetilde{g_m}} M, \qquad (6.31)$$

where M - mantissa of a number.

For retaining/preserving/maintaining the greatest possible accuracy of a number in representation (6.31) the value of mantissa must be limited from below in such a way as to make impossible further decrease of orders, in other words so that would occur the condition

$$p_{n+j} M > \mathcal{P},$$
$$j = 1, 2, \ldots, m. \qquad (6.32)$$

Determination. Under the floating point number representation in the residual classes we will understand the representation, which satisfies condition (6.32). In other words the mantissa of a number of normal form must satisfy the inequalities

$$\frac{\mathcal{P}}{p_j} < M < \mathcal{P}. \qquad (6.33)$$

Page 368.

For the regulated system of bases/bases value j can be selected from

set j=1, 2, ..., n, n+1. However, the set of the possible values j
can be abbreviated/reduced, taking into account the following
considerations. Number A is represented in the expanded range on
further bases/bases p_{n+j} $(j = 1, ..., m)$ only in the arithmetic unit. In
the remaining devices/equipment of machine the mantissa is
represented only on bases/bases p_1 p_2, ..., p_n, therefore selection j=n+1
is unsuitable, since this will hinder/hamper the determination of the
form of the representation of a number in these devices/equipment.
From the remaining possible values of j it is expedient to select the
greatest value of j=n, since in this case the condition

$$\frac{\mathscr{P}}{p_n} \leqslant M < \mathscr{P} \qquad (6.34)$$

satisfies a great quantity of the possible values M, and also,
therefore, more rarely appears need in the number normalization.

If entire numerical range $[0, \mathscr{P})$ is decomposed on p_n intervals,
then condition (6.34) is equivalent to requirement so that the
mantissa of number represented with a floating point would be placed
in any interval

$$[j\mathscr{P}, (j+1)\mathscr{P}),$$
$$j = 1, 2, ..., p_n - 1,$$

except the first, for which j=0.

Continuing the development of the form of the representation of
a number examined, it is possible to construct the new type of the

arithmetic unit, which uses with the integers, but automatically
which corrects the value of the range of the representation of
operands and result, i.e., here from the concept of floating point we
pass to the concept of the floating range of the representation of
numbers.

Page 369.

§ 6.7. Principles of the construction of the combined
discrete-continuous devices/equipment in the system of residual
classes.

An increase in the accuracy of digital computers is limited, in
essence, by the permitted value of discharge nets of machine, i.e.,
by a quantity of equipment, while the accuracy of analog computers in
many respects is determined by quality, in other words in the
precision of equipment, in connection with which accuracy into three
or four accurate sign of result it is considered for them as the
sufficiently high.

Very essential is this factor, as the universality of digital
computers, i.e., the possibility to solve the problems of different
classes without the equipment reconstruction of machine.

The advantages of the digital computers over analog ones are
such essential ones that deficiencies/lacks their, such, as a
quantity and the overall sizes of equipment, the high required
powers, the longer time of the solution of problems, the prolonged
preliminary preparation of tasks for the solution, high qualification
and relatively larger staff of the service personnel, do not
interfere with digital computers to successfully compete with the
analog ones almost in all fields of application of the latter.

Is hence clear interest in the research of discrete-continuous
type hybrid constructions/designs, which, supposedly, could join
advantages of both types of machines, but namely ensure the high
accuracy of the solutions of digital computers with the inherent in
them relatively low requirements for the allowances of the utilized
parts, simplicity, compactness, efficiency/cost-effectiveness, speed
of obtaining result and with the organically inherent in analog
computers ability to work in real time.

It is logical that, remaining in the analog technology at the
level of the ordinary representation of numerical values and diagram
of the solution of problem, we can increase the accuracy of the
solution only due to the considerable decrease of an error in the
equipment, which is possible in the sufficiently limiting limits.

Therefore for an increase in the accuracy of the solution it is considered by advisable to find this form of the representation of numerical values, when each value from the full/total/complete range is represented by the set of numbers of the small numerical ranges. Then, treating individually each value of a small range on the maximum scale of device/equipment and composing at the output/yield the results of processing, we obtain a considerable increase in the accuracy of computer operation.

Page 370.

One of similar methods is the so-called "stretching method", which provides for the separation of input data into the individual parts and processing each part individually in the maximum range of device/equipment.

However, this method is also limited from the point of view of obtaining the high accuracy of result. A most essential deficiency/lack in this method is the need for the account of the connections between the individual parts of the workable values with the execution of operation.

In connection with that presented for solving stated problem of it is expedient to take this form of the representation of numerical

values, when an initial number would be represented by the set of the not connected numbers of small ranges. As we already could be convinced, this requirement satisfies the system of residual classes.

Actually/really, since the remainders/residues on the different bases/bases are not connected, there is no limitation, superimposed by the need for considering the connections between them. Since the result of any rational operation above each digit of the number, represented in the form of remainders/residues along the selected system of bases/bases, itself is remainder/residue on the same bases/bases, then there is no need for scale change in resolving task.

Let us suppose we should to solve some task (for example, find the solution of the system of differential equations) whose numerical values are changed in the range $[0, \mathscr{P})$.

The participating in the solution of problem numerical values are represented in the system of residual classes with range $[0, \mathscr{P})$ in the form of the remainders/residues

$$\alpha_1, \alpha_2, \ldots, \alpha_n$$

on the appropriate bases/bases, each of which is treated on appropriate elementary analog unit $A\mathcal{Y} \ (\mathrm{mod}\ p_1), \ A\mathcal{Y} \ (\mathrm{mod}\ p_2), \ \ldots, \ A\mathcal{Y} \ (\mathrm{mod}\ p_n)$, as this shown in Fig. 6.49.

Thus, treating independently values, greatest of which does not exceed p_n, actually we use with the value, which lies in the range $(0, \mathcal{P})$.

As long as the problem is not completely solved, the described work can be produced independently for each of the analog units $AY(\bmod p_1)$, $AY(\bmod p_2) \ldots$, $AY(\bmod p_n)$, ranges of which are p_1, p_2, $\ldots$, p_n respectively.

Page 371.

It is logical that the input values also are represented in the form of remainders/residues on bases/bases p_1, p_2, $\ldots$, p_n and in this form enter the input of the analog units Vkh1, Vkh2, ..., Vkhn. When processing numerical information in each of the elementary analog units is completed and will come up the question about the output of result, output device VU, after obtaining the value of output quantity in the form of remainders/residues a_1, a_2, $\ldots$, a_n, relating to one and the same moment of time, converts on one of the methods of transition from residual numbers to the positional numeration system the obtained result into a positional number and it will transmit it to the output/yield.

The procedure of readout indicated can be carried out as many once in the time, as is required according to the conditions of task.

Thus, the incoherence between themselves of remainders/residues on the different oases/bases ensures the carrying out of computational process in the free devices/equipment, which work on the different bases/bases, and the need for the transformation of result into its positional form of representation appears already out of the elementary computers.
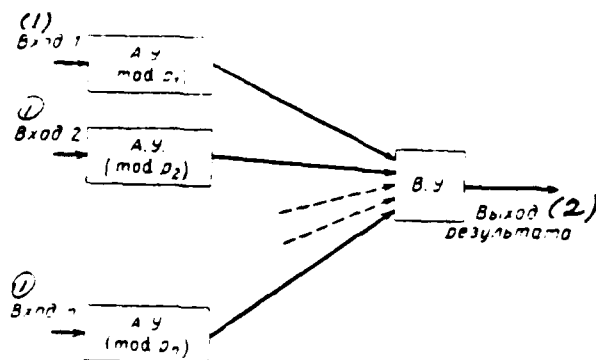
Fig. 6.49. Block diagram of discrete-continuous device/equipment.

Key: (1). input. (2). output of result.

Page 372.

Thus, although each of the devices/equipment must have for the correct determination of the value of numerical value only accuracy of order $\frac{1}{p_i}$ ($i = 1, 2, \ldots, n$), nevertheless under these conditions output result will be determined with an accuracy to value

$$\frac{1}{\mathcal{P}} = \frac{1}{\prod\limits_{i=1}^{n} p_i}.$$

In other words if it proves to be possible to organize elementary analog units, each of which works on modulus/module p_i, then is opened/disclosed the possibility of the construction of the analog system, which works with any preassigned accuracy.

In this case the growth of the accuracy of this analog system will be produced as in the digital computers, only due to an increase in the quantity relative to nonprecision equipment - the addition of certain quantity of elementary analog units, which work in bases/bases $p_{n+1}, p_{n+2}, \ldots, p_{n+k}$, by mutually simple both between themselves and with the previously selected bases/bases.

Passing in the elementary analog unit to the work on basis/base p_i, we build-in into the work of this device/equipment the element/cell of discreteness, which consists in the requirement of the integrality (taking into account scale) of the value of function at this integral (taking into account scale) value of argument.

A similar discreteness is equivalent to substitution by curved broken line, the nearer that approaching curve, the less the step/pitch of separation Δx.

In other words, after assigning the required accuracy of the representation of the curve $y=f(x)$, always it is possible to find such step/pitch of separation Δx, with which the values of function at fixed/recorded points $x_1, x_2, \ldots, x_i$ are known to us with the preset accuracy.

In this sense the discreteness of curve can be treated as

follows. We fix/record the points at which the values of function are known to us with the preset accuracy. Between these points the function varies continuously, but we do not have information about what values it takes. The assignment to function $y=f(x)$, for example, of basis/base p_i also does not break its continuity in the range $[0, p_i)$, since the latter is equivalent to the parallel translation of the axis of abscissas to values $p_i, 2p_i, 3p_i, \ldots$ respectively.

Page 373.

A similar assignment to function ensures correct work of elementary analog unit with the execution of rational operations, that is the latter they are performed by analog unit for each point of curve, and integral (to scale) result is removed/taken, at those values of argument, at which are determined the fixed/recorded points of input function (integral). Since in the system of residual classes any rational operation is accomplished accurately, then at the fixed values of argument the result of any operation is obligated to be integral and deviation from the integrality can be caused only by a equipment error in the device/equipment. Therefore with the deviation of result from the integer value at the fixed values of argument as the accurate value of result must be accepted near integral (to scale) value.

If elementary analog units have a range of a change in values D and one of them works on basis/base p_i, then weight m of unit interval will be defined as $m = \frac{D}{p_i}$. If we proceed from the fact that is permitted an error in result on the order of 1/3 unit intervals, then the permissible relative error δ can be evaluated as

$$\delta = \frac{30}{p_i} \%.$$

Then when selecting of bases/bases among mutually prime numbers 3, 5, 7, 11, 13, 17, 19, 23, 39, 31, which close the range

$$\mathscr{P} \approx 10^{11}.$$

it is possible to use the elementary analog units whose resulting accuracy the order

$$\eta \approx 1 \div 10\%.$$

Page 374.

If under the price of the unit of range M we will understand the ratio of the value of numerical K-band the range of a change in the electrical parameters of device/equipment D, then in the case of using one device/equipment for the work with numerical values, which lie in the range $[0, \mathscr{P})$ we will obtain the price of the unit of the range

$$M_1 = \frac{\mathscr{P}}{D}.$$

and in the case of work on bases/bases $p_1, p_2, \ldots, p_n$ for independent foundation p_i we obtain

$$M_2 = \frac{p_i}{D}$$

whence it follows that the price of the unit of range is reduced

$$\frac{M_1}{M_2} = \frac{\mathscr{P}}{p_i} = \prod_{\substack{j=1 \\ j \neq i}}^{n} p_j \quad \text{times.}$$

Let be now preset function S(x) of the form

$$S(x) = \sum_{k=1}^{n} a_k f_k(x), \qquad (6.35)$$

where a_k— whole non-negative numbers, and f_k— continuous functions, which take the integral (to scale) values at the integral (to scale) values of the argument

$$x_1, x_2, \ldots, x_m,$$

moreover

$$x_m - x_{m-1} = x_{m-1} - x_{m-2} = \ldots = x_2 - x_1.$$

On the strength of the fact that (6.35) is correct for all x it is possible to write

$$S(x_j) = \sum_{k=1}^{n} a_k f_k(x_j) \pmod{p_i},$$

where j=1, 2, ..., m, or

$$S(x_j) = \sum_{k=1}^{n} a_{k_i} f_{k_i},$$
$$j = 1, 2, \ldots, m, \qquad (6.36)$$

where

$$a_{k_i} - a_k \pmod{p_i},$$
$$f_{k_i} = f_k(x_j) \pmod{p_i}.$$

Let us show corectness of transition from (6.35) to (6.26) for some forms of the function $f_k(x)$.

Page 375.

Let $f(x)$ be the function, obtained under the influence of certain operator F on the function $\phi(x)$, i.e.

$$f(x) = F\varphi(x).$$

Then under the assumptions made above we have

$$f_{k_i} = F\varphi_{k_i}.$$

Let us consider the form of operator F for the operations, realized in the residual classes.

For the operation of addition (subtraction)

$$f_k(x) = F_1\varphi_k(x) = \varphi_1(x) - \varphi_2(x).$$

where $\phi_1(x)$ and $\phi_2(x)$ - the function of operands.

On the strength of the fact that at points $x_1, x_2, \ldots, x_m$ we use with the integer values of functions, the remainder/residue of the sum must be equal to the sum of the remainders/residues of components/terms/addends. Hence

$$f_{k_i} = F_1\varphi_{k_i} = \varphi_{1i} + \varphi_{2i},$$
$$i = 1, 2, \ldots, m.$$

For the operation of the multiplication

$$f_k(x) = F_2\varphi_k(x) = \varphi_{1x}\varphi_{2x}.$$

For the integer values the remainder/residue of product, as is known, it is equal to the product of the remainders/residues of

operands, i.e.

$$f_{k_i} = E_2 \varphi_{k_i} = \varphi_{1_i} \varphi_{2_i}.$$

For the operation of the differentiation

$$f_k(x) = F_3 \varphi_k(x) = \frac{d}{dt} \varphi_k(x).$$

or regarding

$$f_k(x) = \frac{\varphi_k(x - \Delta x) - \varphi_k(x)}{\Delta x} + W.$$

where W - member of the second order of smallness.

Choosing along the axis of abscissas scale grid in such a way that $\Delta x = 1$, and examining only the integer values of functions, it is possible to write

$$f_{k_i} = F_3 \varphi_{k_i} = \varphi_{k_i}(x_j + 1) - \varphi_{k_i}(x_j).$$

For the operation of the integration

$$f_k(x) = F_3 \varphi_k(x) = \int_{x_0}^{x} \varphi_k(x)\, dx.$$

Page 376.

Since the integral can be represented in the form of the sum of products and since the step/pitch of integration can be combined with the step/pitch of scale grid along the axis of abscissas, then it is correct

$$f_{k_i} = \int_{x_0}^{x} \varphi_{k_i}\, dx.$$

Thus, is established/installed the fact that for the operations examined expression (6.35) can be substituted by expression (6.36).

This is correct under the done above assumption that at the points of the selected scale grid along the axis of abscissas function-operands accept the strictly integral (to scale) values.

Let us consider now the situation when function-operands ϑ_1 and ϑ_2 under the effect of some factors deviated by values ε_1 and ε_2 from their integer values. Since the result must be integral, then it is necessary it to correct, after relating to the nearest integer value. Therefore, obviously, errors in function-operands and error in the device/equipment, which performs above them the preset operation, must be in this state that the result would be obtained near the true integer value, and then at the output/yield of elementary analog circuit must be connected the device/equipment, which corrects the value of output function at points $x_1, x_2, \ldots, x_m$ to the nearest integer value. If series-connected several elementary analog units, then compensator must be connected only in that place, where accumulated error for result, which is obtained due to an inaccuracy in the previous devices/equipment, becomes close to the critical.

As the illustration, let us consider the integration of linear differential equation with the constant coefficients.

Example. Let us consider work of the elementary analog unit, which has error not better than 1c/c, the realizing the solution

differential equation

$$\frac{dx}{dt} = x \qquad\qquad (6.37)$$

with the initial condition $x(t=0) = x_0$ with an accuracy to k signs.

For guaranteeing the integrality of argument let us introduce the scale, determined from the condition

$$M_t \Delta t = 1.$$

Page 377.

Then the range of a change of the argument to scale is represented as $(0, M_t T)$.

Let us introduce scale M_x, ensuring the integrality of function in the preset range of argument, in the form $M_x = 10^k$, for obtaining the accuracy in k of decimal points after comma. Let us select bases/bases $p_1, p_2, \ldots, p_n$ from the condition

$$\mathcal{P} = \prod_{i=1}^{n} p_i \geqslant M_x x(t = T).$$

Then the initial condition

$$\widetilde{x}_0 = M_x x_0$$

can be registered in the form

$$\widetilde{x}_0 = (x_{01}, x_{02}, \ldots, x_{0n}).$$

To solve equation (6.37) we will be on all n to bases/bases in parallel, for which it is necessary to have n of the elementary analog units each of which works on their basis p_i $(i = 1, 2, \ldots, n)$ with

initial condition x_{0i}.

Determination. Subsequently the solution of initial equation for basis/base p_i we will call the projection of the solution by this basis/base.

Let us consider the functioning of the device/equipment, represented in Fig. 6.50 on basis/base p with initial condition $x_{0i} = \dot{a}$ from moment/torque t_i. The delay time of the integrating component/link let us designate through τ. Here IZ designates the elementary integrating component/link, KU - compensator, V - input tube. In the time interval $[t_i, t_i - \tau)$ output stress/voltage will be

$$x_1 = a.$$

In interval $[t_i + \tau, t_i + 2\tau)$ we will obtain

$$x_2 = a(1 + (t - t_i) - \tau).$$
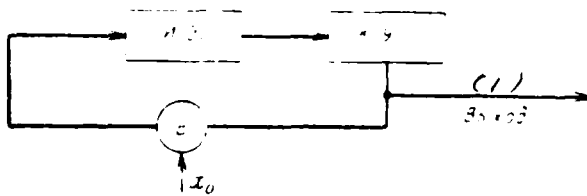
Fig. 6.50. Block diagram of the integrating device/equipment.

Key: (1). output.

Page 378.

For interval $(t_i + 2\tau, t_i + 3\tau)$ we will obtain

$$x_3 = a(1 - \tau)(1 + (t - t_i)) + a\frac{(t - t_i)^2}{2}.$$

For interval $(t_i + 3\tau, t_i + 4\tau)$ —

$$x_4 = a(1 - \tau)\left(1 + (t - t_i) + \frac{(t - t_i)^2}{2}\right) + a\frac{(t - t_i)^3}{3!}.$$

. . . .

For interval $(t_i + n\tau, t_i + (n - 1)\tau)$ we will obtain

$$x_{n+1} = a(1 - \tau)\left(1 + (t - t_i) + \frac{(t - t_i)^2}{2} + \ldots + \frac{(t - t_i)^n}{n!}\right) +$$
$$+ a\tau\frac{(t - t_i)^n}{n!}.$$

Whence

$$x_{n+1} = a(1 - \tau)e^{t - t_i} + a\tau\frac{(t - t_i)^n}{n!}.$$

With an accuracy to the value of the remainder

$$R_n = \frac{(t - t_i)^{n+1}}{(n + 1)!}e^{\Theta(t - t_i)}.$$

where

$$0 < \Theta < 1.$$

Compensator in this case at each fixed/recorded moment of time ensures the integrality of result that it is equivalent to task at this moment of the time of the exact initial values, which exclude the prehistory of the work of device/equipment.

After designating $t - t_i = t_1$, we will obtain

$$x = a(1-\tau)e^{t_1} + a\tau \frac{t_1^n}{n!} + a(1-\tau)R_n. \qquad (6.38)$$

Let us now move on to the numerical computations. Let the initial value of function be is preset as by $x(t=0)=1$. We will seek the solution of equation (6.37) with an accuracy to four signs in the range of argument [0, 1).

Then $M_x = 10^4$ and the solution will take the form

$$x = M_x e^{M_t t'},$$

whence the initial value of function (to scale) $x_0 = 10^4$. Let us select the step/pitch of argument equal to 0.01, then with the introduced scales argument varies in the interval [0, 100) with the step/pitch $\Delta t = 1$, and function - in the interval [10^4, 27 183).

Page 379.

Let us select the system of the bases/bases: $p_1 = 11$, $p_2 = 12$, $p_3 = 13$, $p_4 = 17$. its range $\mathscr{P} = 29172 > 27183$. We compute the values of the orthogonal bases:

$$B_1 = 2652, \quad B_2 = 17017, \quad B_3 = 11220, \quad B_4 = 27456.$$

Initial condition will be registered as $x_0 = (1, 4, 3, 4)$. Scale of argument $M_t = (1, 4, 9, 15)$, the scale of function $M_x = (1, 4, 3, 4)$.

Each value t^k is accompanied by coefficient $\frac{M_x}{M_t^n}$. Here

$$\frac{M_x}{M_t} = (1, 4, 9, 5) = 100, \quad \frac{M_x}{M_t^2} = (1, 1, 1, 1) = 1.$$

$$\frac{M_x}{M_t^k} = (0, 0, 0, 0) = 0 \quad \text{при} \quad k > 2. \quad (1)$$

Key: (1). with.

Considering that $r \ll t$, we will obtain value of x at point $t_1 = 1$:

$$x_1 \,(\text{mod } p_1) = 3, \quad x_1 \,(\text{mod } p_2) = 9, \quad x_1 \,(\text{mod } p_3) = 0, \quad x_1 \,(\text{mod } p_4) = 3.$$

which corresponds in the decimal system to the number

$$x_1 = 3B_1 + 9B_2 + 3B_4 = 10\,101$$

or taking into account scale $x_1 = 1,0101$.

After the carrying out corrections we pass to the point $r = 2$, where we work with the new initial value of function $x_0 = (3, 9, 0, 3)$. Here each value t^k is accompanied by the coefficients:

$$\frac{M_x}{M_t} = (2, 8, 5, 13) = 200, \quad \frac{M_x}{M_t^2} = (2, 2, 2, 2) = 2.$$

$$\frac{M_x}{M_t^3} = (0, 0, 0, 0) = 0.$$

Then the value of function x at the new point t_2 is defined as

$$x_2 \,(\text{mod } p_1) = 5, \quad x_2 \,(\text{mod } p_2) = 2, \quad x_2 \,(\text{mod } p_3) = 10, \quad x_2 \,(\text{mod } p_4) = 2.$$

Whence $x = (5, 2, 10, 2) = 10\,202$ or to scale $x = 1,0202$.

Thus can be obtained the values of the unknown function at other values of argument.

Page 380.

Chapter 7.

SYSTEM OF RESIDUAL CLASSES IN COMPLEX DOMAIN.

In his famous "arithmetic research" K. F. Gauss builds-in into
the examination complex integers a+bi, where a and b - whole real
numbers, and is constructed the theory of comparisons for complex
integers. We is presented further, following Gauss, some necessary
for future reference questions of the arithmetic of such complex
integers. Everywhere further under a complex number we will
understand complex integer, if contrary will not be in a special
manner stipulated.

It is easy to see that the sum, difference and product of two
complex integers is also complex integer. Let $\dot{A}=a+bi$ - certain
complex number. The numbers
$$\dot{A}(-1) = -a-bi, \quad \dot{A}i = ai-b, \quad \dot{A}(-i) = -ai+b,$$
the obtained by multiplication numbers $\dot{A}$ respectively on -1, i, -i,
are the associated with $\dot{A}$ numbers. Number $\overline{\dot{A}}$, formed from $\dot{A}$ by

replacement in it i on -i, is the conjugated/combined with $\dot{A}$ number. Value

$$N_A = \dot{A}\overline{\dot{A}} = (a + bi)(a - bi) = a^2 + b^2$$

is called the norm of number $\dot{A}$, and also number $\overline{\dot{A}}$.

Page 381.

A complex number will be called prime complex number, if it cannot be represented in the form of the product of two complex numbers, different from unity. Otherwise it is called a composite/compound complex number.

From this determination it directly follows that composite/compound real number is also a composite/compound complex number. Reverse is not always correct: simple real number can be a composite/compound complex number. Thus, for instance, $2 = (1+i)(1-i)$.

Is analogous, any prime number of form $4k+1$ $(k>0)$ which, as is known from the theory of numbers, it can be decomposed on the sum of two squares, it is a composite/compound complex number. For example,

$$29 = 4 \cdot 7 + 1 = (5 - 2i) \cdot (5 - 2i); \quad 37 = 4 \cdot 9 + 1 =$$
$$= (6 + i)(6 - i) \text{ и т. д. } (1)$$

Key: (1). and so forth.

As far as numbers are concerned prime of form $4k+3$, then they cannot be represented in the form of the sum of two squares and therefore they are prime complex numbers.

For complex numbers can be isolated some concepts, inherent in whole real numbers, for example this important concept as parity or oddness. Here as the composite "pair" comes forward a number $1+i$. The complex number $a+bi$ is odd, if it is not divided into $1+1i$. The complex number $a+bi$ is even, if a and b are even; in this case it is always divided into $1+1i$. Besides these two classes of complex numbers is an intermediate class of the numbers, which separate on $1+i$, but which have a and b - odd numbers. This intermediate class Gauss calls semiaven complex numbers.

For of the introduced thus complex integers occurs the theorem about the uniqueness of the disintegration of a composite/compound complex number into its simple cofactors.

In accordance with this here, naturally, is defined the concept of mutually prime complex numbers as such numbers in expansions of which into the simple cofactors there are no common factors, besides unity.

Page 382.

§ 7.1. Comparison complex integers.

The complex number $\dot{A}=a+bi$ will be multiple to the complex number $\dot{m}=p+qi$ (or m it will be the divider/denominator of number $\dot{A}$), if the quotient $\dot{A}:\dot{m}$ is a complex number [1].

FOOTNOTE [1]. We recall that under a complex number we always have in mind complex integer. ENDFOOTNOTE.

In other words since

$$\frac{\dot{A}}{\dot{m}} = \frac{a-bi}{p+qi} = \frac{(a-bi)\cdot(p-qi)}{p^2+q^2} = \frac{ap-bq}{p^2+q^2} + \frac{bp-aq}{p^2+q^2}i.$$

that $\dot{A}:\dot{m}$ will be integer in that and only when

$$ap - bq \equiv 0 \,(\mathrm{mod}\, p^2 + q^2),$$
$$bp - aq \equiv 0 \,(\mathrm{mod}\, p^2 + q^2). \qquad (7.1)$$

If (7.1) it is not performed, then $\dot{A}$ is not divided into $\dot{m}$. let $\dot{S}=e+fi$ be such, which $\dot{A}-\dot{S}$ is divided into $\dot{m}$, then it is possible to write that

$$\dot{A} \equiv \dot{S}\,(\mathrm{mod}\,\dot{m}), \qquad (7.2)$$

or $\dot{S}$ is deduction $\dot{A}$ on modulus/module $\dot{m}$.

Example. To determine the fissionability of numbers $\dot{A}=17+7i$, $\dot{m}=3+2i$. Here $p^2+q^2=9+4=13$; $ap+bq=17 \cdot 3+7 \cdot 2=51+14=65$;

$bp-aq=7 \cdot 3-2 \cdot 17=-13$.

Conditions (7.1) are satisfied: $65 \equiv 0$ (mod 13); $-13 \equiv 0$ (mod 13).

Theorem 7.1. Let $\dot{A}=a+bi$, $\dot{m}=p+qi$ be performed the comparisons

$$ap + bq \equiv xp + yq \;(\text{mod}\, p^2 + q^2),$$
$$bp - aq \equiv yp - xq \;(\text{mod}\, p^2 + q^2). \qquad (7.3)$$

Then

$$\dot{A} \equiv x + iy \;(\text{mod}\, \dot{m}).$$

Page 383.

Proof. We divide number $\dot{A}-(x+iy)$ into $\dot{m}$

$$\frac{\dot{A}-(x+iy)}{\dot{m}} = \frac{(a-x)+i(b-y)}{p+qi} = \frac{(a-x)\cdot p-(b-y)\cdot q}{p^2-q^2} +$$
$$+ \frac{(b-y)\cdot p-(a-x)\cdot q}{p^2+q^2}\, i.$$

So that as a result of division would be obtained a complex number they must take the place of the comparison

$$(a-x)\, p + (b-y)\, q \equiv 0 \;(\text{mod}\, p^2 - q^2),$$
$$(b-y)\, p - (a-x)\, q \equiv 0 \;(\text{mod}\, p^2 - q^2).$$

which were equivalent (7.3).

Thus, with execution (7.3) number x+iy is the deduction of number $\overset{\bullet}{A}$ on modulus/module $\overset{\bullet}{m}$.

Although for complex numbers are not determined the concepts "more" and "it is less" however it is the possible to determine the concept of the smallest deduction. The basic idea of this determination lies in the fact that since the determination of composite deduction is based on the system of real comparisons (7.3), then, after requiring so that xp+yq and yp-xq they would be respectively smallest deductions on modulus/module p^2+q^2, we will obtain completely specific complex number x+iy, which it is logical to name the smallest deduction of number $\overset{\bullet}{A}$ modulo $\overset{\bullet}{m}$. In other words it is assumed that

$$xp+yq \leqslant p^2+q^2-1.$$
$$yp-xq \leqslant p^2+q^2-1.$$

In this case should be distinguished the smallest deductions and the least positive residues. In the first case it is assumed that xp+yp and yp-xq are positive integer numbers, exceeding p^2+q^2-1. In the second case it is assumed that these values can be both positive and negative ones, but those not exceeding in the absolute value of number $p^2+q^2/2$.

If are found the smallest deductions of expressions ap+bq and bp-aq

$$r \equiv ap + bq \,(\mathrm{mod}\, p^2 - q^2),$$
$$r' \equiv bp - aq \,(\mathrm{mod}\, p^2 - q^2). \qquad (7.4)$$

then the smallest deduction of number $\overset{\bullet}{A}$ on modulus/module $\overset{\bullet}{m}$ is equal to

$$x + iy = \frac{rp - r'q}{p^2 + q^2} + \frac{r'p - rq}{p^2 + q^2}\, i. \qquad (7.5)$$

Page 384.

Example. To determine the smallest deduction of number $\overset{\bullet}{A}=15+2i$ on modulus/module $\overset{\bullet}{m}=3+2i$. Let us write the system of comparisons (7.3) under conditions of the example

$$49 \equiv 3x + 2y \,(\mathrm{mod}\, 13),$$
$$-24 \equiv 3y - 2x \,(\mathrm{mod}\, 13).$$

Hence we obtain the equations

$$3x + 2y = 10,$$
$$-2x + 3y = 2.$$

Solution of this system gives x=2, y=2, i.e., 2+2i there is the unknown smallest deduction.

Example. Under conditions of the previous example to find the least positive residue. System of equations for determining of x and

y in this case will take the form

$$3x + 2y = -3,$$
$$-2x + 3y = 2.$$

The solution of this system will be x=-1, y=0, i.e., -1 unknown least positive residue.

The properties of comparisons for the real region extend also to complex domain; therefore we on them stop will not be.

If complex numbers are not mutually simple, then they have common divisors. Here also it is possible to introduce the concept of greatest common divisor as common divisor with the greatest norm. The process of the determination of the greatest common divisor of two complex numbers $\overset{\bullet}{A}_1$ and $\overset{\bullet}{A}_2$ is analogous used for the determination of the greatest common divisor in the real case.

§ 7.2. Fundamental theorem of Gauss.

Now we approached one of the most interesting and important questions of the theory complex integers - to the determination of the class of the smallest deductions and this connected with theorem of Gauss about the isomorphism between the sets of real and complex numbers.

Page 385.

Determination. If two sets it is possible then mutually
idetically is mapped one to another so that the specific in them
relationships/ratios during the representation would not be broken,
i.e., if to each element/cell a from set X it is possible to mutually
unambiguously relate element/cell $\bar{a}$ from set $\bar{X}$, then so that the
relationships/ratios, which exist between any elements/cells
a,b,c,d.. from X, would occur, also, between equivalent components
$\bar{a},\bar{b},\bar{c},\bar{d}$... from $\bar{X}$ and vice versa, then these sets are called
isomorphic.

In the previous paragraph we established that the smallest
deduction of any complex number a+bi on the composite modulus/module
p+qi is determined, on the basis of the system of two real
comparisons

$$ap \div bq \equiv r \,(\mathrm{mod}\, p^2 \div q^2),$$
$$bp - aq \equiv r' \,(\mathrm{mod}\, p^2 + q^2),$$

(7.6)

where r and r' - smallest posit.ve deductions on the real
modulus/module $N = p^2 + q^2$. Since for r and r' are possible values of
0.1,... N-1, then it could at first glance seem that the smallest
composite deductions there can be N^2, the obtained during different
combinations values r and r'. However, this not thus. Values r and r'
are not not depended. Between them there is a specific connection,

which sets in the conformity to each possible value of r completely specific value r'. Let us establish this connection. Multiplying the first of comparisons (7.6) on p, and the second - on q and by subtracting the second comparison from the first, we will obtain

$$a(p^2 + q^2) \equiv rp - r'q \, (\mathrm{mod}\, p^2 + q^2)$$

or

$$r'q \equiv rp \, (\mathrm{mod}\, p^2 + q^2). \qquad (7.7)$$

If p and q - mutually prime numbers, then comparison (7.7) has one solution

$$r' \equiv tr \, (\mathrm{mod}\, p^2 + q^2),$$

where

$$t = \frac{p + z(p^2 + q^2)}{q},$$

moreover z is such that t - whole less than $p^2 + q^2$.

We illustrate the aforesaid by an example.

Example. To determine all possible pairs of values r and r' with modulus/module p+qi=3+4i.

Page 386.

Since 3 and 4 mutually prime numbers, then in this case and comparison (7.7) has a solution

$$t = \frac{3 + 1 \cdot 25}{4} = 7$$

$$r' \equiv 7r \pmod{25},$$

which determines the following pairs of values r and r'

(0, 0); (1, 7); (2, 14);
(3, 21); (4, 3); (5, 10); (6, 17); (7, 24); (8, 6); (9, 13); (10, 20); (11, 2);
(12, 9); (13, 16); (14, 23); (15, 5); (16, 12); (17, 19); (18, 1); (19, 8);
(20, 15); (21, 22); (22, 4); (23, 11); (24, 18).

The considerations presented feed us to the remarkable theorem of Gauss.

Theorem 7.2. (Fundamental theorem of Gauss I). On the preset composite modulus/module $\dot{m}=p+qi$, whose norm is equal to $N=p^2+q^2$, also, for which p and q are mutually prime numbers, each complex integer is congruent with one and only by one deduction of the series/row

$$0, 1, 2, 3, \ldots N-1.$$

Proof. It is known from the theory of numbers, that for two mutually prime numbers p and q it is possible to find such two integers u and v, that

$$up + vq = 1. \qquad (7.8)$$

Let us write the easily checked identity

$$i = uq - vp + \dot{m}(v + ui). \qquad (7.9)$$

Let be is given the complex number a+bi. Let us rewrite it, after replacing i from (7.9)

$$a + bi = a + (uq - vp) \cdot b + \dot{m}(vb + ubi).$$

Let us designate through h the smallest positive real deduction of number a+(uq-vp)b on modulus/module N and let us assume that

$$a + (uq - vp) b = h + sN = h + s(p + qi)(p - qi) - $$
$$= h + \dot{m}(ps - qsi).$$

Then will be performed the equality

$$a - bi = h + \dot{m}\,(ps - qsi) - \dot{m}\,(vb - ubi) =$$
$$= h + \dot{m}\,[ps - vb + (ub - qs)\,i]$$

or in the form of the comparison

$$a - bi \equiv h \,(\mathrm{mod}\,\dot{m}). \qquad (7.10)$$

Page 387.

By this it is proved that a+bi is congruent with one of the numbers 0, 1,2... N-1 in modulus/module $\dot{m}$. Let us demonstrate now that this number is unique. Let us assume that occur two comparisons

$$a - bi \equiv h_1 \,(\mathrm{mod}\,\dot{m}),$$
$$a - bi \equiv h_2 \,(\mathrm{mod}\,\dot{m}).$$

According to the property of the comparisons of number h_1 and h_2 they are congruent between themselves in modulus/module $\dot{m}$, i.e.,

$$h_1 \equiv h_2 \,(\mathrm{mod}\,\dot{m})$$

or

$$h_1 - h_2 \equiv 0 \,(\mathrm{mod}\,\dot{m}),$$

i.e.

$$h_1 - h_2 = \dot{m} \cdot (e + fi). \qquad (7.11)$$

From (7.11) it follows that will be carried out the equality

$$(h_1 - h_2) \cdot (p - qi) = N \cdot (e - fi).$$

which is equivalent to the following two real equalities:

$$(h_1 - h_2) \cdot p = Ne,$$
$$(h_1 - h_2) \cdot q = -Nf. \qquad (7.12)$$

After multiplying first equality (7.12) on u and the second on v and after forming them, we will obtain

$$(h_1 - h_2)(up + vq) = N(eu - fv),$$

whence, taking into account (7.8), it follows

$$h_1 - h_2 = N(eu - fv)$$

or

$$h_1 - h_2 \equiv 0 \pmod{N}. \qquad (7.13)$$

Since by hypothesis $h_1 < N$ and $h_2 < N$, then (7.13) it is possible only in the case of $h_1 = h_2$.

Thus, is rejected the possibility of the existence of two numbers h_1 and h_2, smaller N which they would be congruent with a+bi in modulus/modula m. There is only one such number which is determined from the comparison

$$a + (uq - vp)b \equiv h \pmod{N} \qquad (7.14)$$

or

$$a + b\rho \equiv h \pmod{N}.$$

Page 388.

This theorem sets the isomorphism between complex numbers and
their real deductions, determined by form indicated above.

Determination. Expression uq-vp, by means of which is
established a correspondence between the composite and real deduction
on modulus/module p+qi, let us name the coefficient of isomorphism
and let us designate it through ρ.

Example. To solve comparison $16+7i \equiv h \pmod{5+2i}$. Since $(5.2)=1$,
condition of theorem 7.2 is satisfied, therefore, there is a
full/total/complete system of real deductions. Here the coefficient
of the isomorphism of modulus/module 5+2i is equal to

$$\rho = uq - vp = 2 \cdot 1 - 2 \cdot 5 = 12, \text{ так как } up + vq = 1 \cdot 5 - 2 \cdot 2 = 1.$$

Key: (1). since.

Therefore $16+7 \cdot 12 \equiv h \pmod{29}$, whence $h=13 \pmod{29}$. Consequently,

$$16 + 7i \equiv 13 \pmod{5+2i}.$$

Relying on this theorem it is possible to show the validity of the
following: let for two numbers $\dot{A_1} = a_1 + b_1 i$ and $\dot{A_2} = a_2 + b_2 i$ there be such
h_1, h_2, $h_\pm$ and h_x, that

$$\dot{A_1} \equiv h_1 \pmod{\dot{m}}, \quad \dot{A_2} \equiv h_2 \pmod{\dot{m}},$$
$$\dot{A_1} \pm \dot{A_2} \equiv h_\pm \pmod{\dot{m}}, \quad \dot{A_1} \cdot \dot{A_2} \equiv h_x \pmod{\dot{m}};$$

then

$$h_\pm \equiv h_1 \pm h_2 \,(\mathrm{mod}\,N), \ \ h_\times \equiv h_1 \cdot h_2 \,(\mathrm{mod}\,N),$$

where N - norm $\dot{\mathbf{n}}$.

Let us return to comparison (7.7). Until now, were examined the
solution of this comparison and the theorem of Gauss under the
condition when p and q - mutually prime numbers. let us consider the
now general case when p and q, and therefore, and $N=p^2+q^2$ have common
factor.

Page 389.

Let us designate it through d. We obtain p=ed, q=fd,
$N=(e^2+f^2)d^2$. In accordance with the theory comparison (7.7) in this
case will have i of the solutions of the following form:

$$r' \equiv \alpha \,(\mathrm{mod}\,N), \ \ r' \equiv \alpha + \frac{N}{d}\,(\mathrm{mod}\,N), \ \ r' \equiv \alpha + \frac{2N}{d}\,(\mathrm{mod}\,N)\dots,$$
$$\dots, r' \equiv \alpha + \frac{(d-1)N}{d}\,(\mathrm{mod}\,N), \qquad (7.15)$$

where $\alpha < N/d$ satisfies the comparison

$$fr' \equiv er \,(\mathrm{mod}\,(e^2+f^2)\,d), \qquad (7.16)$$

in which is already carried out the condition of mutual simplicity e
and f and solution of which is obtained by already known path.

Example. To determine all possible pairs of values r and r' with p+qi=3+6i.

Comparison (7.7) under the condition of an example takes the form

$$6r' \equiv 3r \ (\text{mod } 45).$$

Here the common factor d=3. Comparison (7.16) is such

$$2r' \equiv r \ (\text{mod } 15).$$

This comparison has a solution

$$r' \equiv 8r \ (\text{mod } 15).$$

Thus, we have the following three groups of the solutions:

$$r' \equiv 8r \ (\text{mod } 45), \ r' \equiv 8r + 15 \ (\text{mod } 45). \ r' \equiv 8r + 30 \ (\text{mod } 45).$$

Let us give the table of all pairs (r',r).

the 1st group

(0, 0); (1, 8); (2,16); (3, 24); (4,32); (5, 40); (6, 3), (7,11); (8,19);
(9,27); (10,35); (11, 43); (12, 6); (13, 14); (14, 22)

the 2nd group

(0, 15); (1, 23); (2, 31); (3,39); (4, 2); (5, 10); (6, 18); (7, 26); (8,34);
(9,42); (10, 5); (11, 13); (12, 21); (13,29); (14,37)

the 3rd group

(0, 30); (1, 38); (2, 1); (3, 9); (4, 17); (5,25); (6,33); (7, 41); (8,4);
(9, 12); (10, 20); (11, 28); (12, 36); (13, 44); (14, 7)

Just as in the case of mutual simplicity p and q the total
quantity of different ones vapor r' and r is equal to N.

Let us formulate now the theorem of Gauss in general.

Theorem 7.3. (Fundamental theorem of Gauss II). On the composite
modulus/module $\dot{m}$=p+qi whose norm N=p²+q² and for which p and q has
the greatest common divisor d>1, each complex integer a+bi is
congruent with deduction x+iy, which possesses that property, what x
is one of the numbers 0, 1.2,... N/d - 1, and y - one of the numbers
0, 1.2,... d-1, moreover only with one only of all N of the
deductions, which have this form.

Page 390.

Let us note that for the modulus/module with the not mutually
simple components no longer occurs the isomorphism with real numbers.
Here the theorem of Gauss sets the smallest deductions of numbers
a+bi in the form of the complex numbers x+yi whose components do not
exceed in the value of numbers d and N/i, whatever numbers a and b.
This fact is also very essential.

Values x and y are determined from the relationships/ratios:

$$b \equiv y \,(\mathrm{mod}\,d),$$
$$a - (uq - vp) \cdot \frac{b - y}{d} \equiv x \left(\mathrm{mod}\,\frac{N}{d}\right), \qquad (7.17)$$
$$up - vq = d.$$

Here also it is possible to examine not the smallest positive deductions, but the least positive residues.

Let us consider the execution of arithmetic operations in the class of the smallest and least positive residues. Let us turn to the fundamental theorem of Gauss. In accordance with the established/installed in it isomorphism to each composite smallest deduction x+iy on modulus/module $\dot{m}$=p+qi corresponds the real deduction h on modulus/module N=p²+q². This real deduction is computed from the formula

$$x - (uq - vp) \cdot y \equiv h \,(\mathrm{mod}\,N),$$

where u and v such, that up+vq=1.

Example. To determine the real smallest deductions, which correspond to composite smallest deductions on modulus/module $\dot{m}$=3+4i.

Here

$u = -1, \quad v = 1, \quad uq - vp = -7 \quad -3 + 3i \sim 1, \quad -3 + 4i \sim 19,$
$-2 - 2i \sim 9, \quad -2 - 3i \sim 2, \quad -2 - 4i \sim 20, \quad -2 + 5i \sim 13, \quad -1 - i \sim 17,$
$-1 - 2i \sim 10, \quad -1 - 3i \sim 3, \quad -1 + 2i \sim 21, \quad -1 - 5i \sim 14, \quad -1 + 6i \sim 7,$
$0 - 0i \sim 0, \quad i \sim 18, \quad 2i \sim 11, \quad 3i \sim 4, \quad 4i \sim 22, \quad 5i \sim 15, \quad 6i \sim 8, \quad 1 + 2i \sim 12,$
$1 + 3i \sim 5, \quad 1 + 4i \sim 23, \quad 1 - 5i \sim 16, \quad 2 + 3i \sim 6, \quad 2 + 4i \sim 24.$

In accordance with the results of an example can be constructed

the table of isomorphism.

Analogous tables can be constructed, also, for the operation of addition, multiplication, formal division and generally for any combination of rational operations.

The adjusted by the theorem of Gauss isomorphism for the modulus/module with the mutually simple components makes it possible to replace the execution of the rational operations above the smallest composite deductions executing the same operations above the corresponding to them real deductions on the real modulus/module, equal to the norm of composite modulus/module. In this case from the technical side the execution of the operations above the real deductions can be realized by any arithmetic units both of the tabular type and by adders and unstable type multipliers.

Page 391.

However, as far as modulus is concerned composite whose components contain common factor, then in this case isomorphism does not occur. Meanwhile this does not mean that and here it is not possible the execution of the operations above the composite smallest deductions to replace with the execution of the operations above their real equivalents, for example, above the reference numbers from

1 to N(N - norm), conferred to completely arbitrarily these smallest

deductions. However, this replacement is possible only with tabular

method of procedure, when the table of reference numbers is present,.

$\dot{W}_k$ — smallest composite deduction whose reference number k (k=1,

2,... ,N). let it be further $\dot{W}_{k_1} - \dot{W}_{k_2} = \dot{W}$ (mod $\dot{m}$). Then in the table

of real equivalents in the intersection of line k_1 with column k_2 is

placed number k_3, although, generally speaking, $k_1 + k_2 \neq k_3$. It is

analogous for other rational operations. It is obvious that the

execution of the operations above the real equivalents in unstable

type arithmetic units, which realize the completely specific

conformity between k_1 and k_2, identical for any k_1 and k_2, in this

case is impossible in view of the absence of this conformity which

would be performed for any k_1 and k_2.

Thus, and for the moduli/modules with the mutually not simple

components is possible replacement in the operations of composite

smallest deductions by their real equivalents.

Example. To make table of multiplication above the real

equivalents on modulus/module $\dot{m} = 2 + 2i$.

Let us first of all determine the smallest composite deductions

on the modulus/module $2+2i$. Let us make table of multiplication for

the composite deductions

	1	2	3	4	5	6	7	8
	$-1-i$	$-1-2i$	$0-0i$	$0-i$	$0-2i$	$0-3i$	$1-i$	$i-2i$
1) $-1-i$	$0-2i$	$-1-i$	$0-0i$	$1-i$	$0-0i$	$1-i$	$0-2i$	$1-i$
2) $-1-2i$	$-1-i$	$-1-2i$	$0-0i$	$0-i$	$0-2i$	$0-3i$	$1-i$	$1-2i$
3) $0-0i$	$0-0i$	$0-0i$	$0-0i$	$0-0i$	$0-0i$	$0-0i$	$0-0i$	$0-0i$
4) $0-i$	$1-i$	$0-i$	$0-0i$	$1-2i$	$0-2i$	$-1-2i$	$-1-i$	$0-3i$
5) $0-2i$	$0-0i$	$0-2i$	$0-0i$	$0-2i$	$0-0i$	$0-2i$	$0-0i$	$0-2i$
6) $0-3i$	$1-i$	$0-3i$	$0+0i$	$-1-2i$	$0-2i$	$1-2i$	$-1-i$	$0-i$
7) $1-i$	$0-2i$	$1-i$	$0+0i$	$-1-i$	$0-0i$	$-1-i$	$0-2i$	$1-i$
8) $1+2i$	$1-i$	$1-2i$	$0+0i$	$0-3i$	$0+2i$	$0-i$	$1-i$	$-1-2i$

Page 392.

On the basis of this table let us make table of multiplication in the reference numbers of deductions.

	1	2	3	4	5	6	7	8
1	5	1	3	7	3	7	5	7
2	1	2	3	4	5	6	7	8
3	3	3	3	3	3	3	3	3
4	7	4	3	2	5	3	1	6
5	3	5	3	5	3	5	3	5
6	7	6	3	2	5	8	1	4
7	5	7	3	1	3	1	5	7
8	7	8	3	6	5	4	7	2

Here not noticeably no law. The realization of operation in the real equivalents by reference numbers is possible only by tabular path.

In a similar manner can be comprised the tables of operations,
also, for the least positive residues both in the case of the
mutually simple components of composite modulus/module and when, in
these components, common divisor is present,.

§ 7.3. Full/total/complete system of deductions. Geometric
interpretation.

In the present paragraph will be examined the methods of
obtaining the full/total/complete system of deductions with the
composite modulus/module. Together with the purely arithmetic methods
to here expediently indicate also some geometric constructions, which
lead to obtaining of the full/total/complete system of deductions,
which are based on the geometric interpretation complex integers.

As is known, complex numbers by representative points on the
plane. Let us select the rectangular Cartesian coordinate system with
X and Y axes and unity of scale e and will lead two systems of
straight lines, parallel to axes with respect to X and Y axes and
distant one behind the the parallel to it another at a distance of e.
The origin of coordinates (point of intersection of X and Y axes) let
us designate through O (Fig. 7.1). Then the points of intersection of

these straight lines will represent complex integers.

Page 393.

Along the axis of abscissas will be plotted/deposited the values
of the real parts of the complex number, while along the axis of
ordinates - value of alleged parts. Thus, point M with coordinates
(p,q) represents the complex number p+qi. The straight line OM
represents value $\sqrt{N}$. Norm itself N is represented by the area of the
square, constructed on the straight line OM (square ORLM). Here
OR=OM=RL=LM=$\sqrt{N}$. If entire plane is covered with such squares (carrying
out of the straight lines, parallel respectively OM and OR, at the
distances, $\sqrt{N}$ one from another), then to the apexes/vertexes of these
squares will correspond the numbers, multiple p+qi. Thus, from the
condition of perpendicularity OR and OM it follows that to point R
corresponds a complex number -q+pi and quotient -q+pi/p+qi=i. As a
result of parallelism OM and RL to point L will correspond complex
number (p-q)+(p+q)i and the corresponding quotient will be equally
1+i.
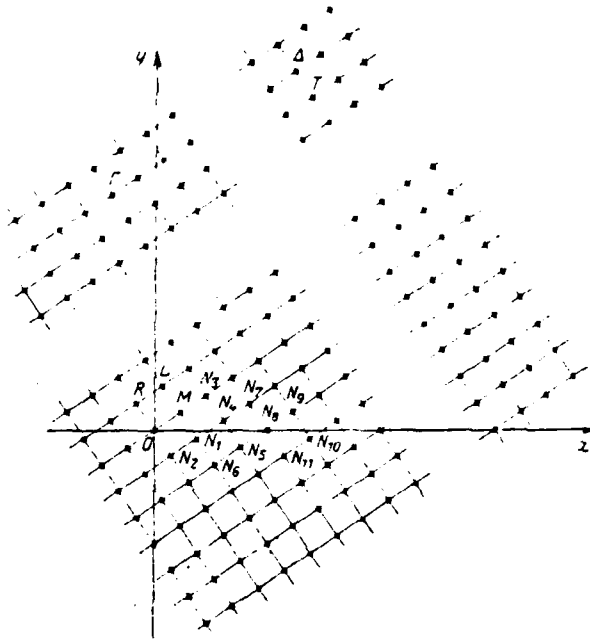
Fig. 7.1. Geometric representation of complex numbers.

Page 394.

Let us number the straight lines, parallel OR and OM, by numbers 0 (straight line OR), 1.2,... ,1, -1, -2,... ,-1 and 0 (straight line OM), 1.2,... ,s, -1, -2,... ,-s.

    Let be given apex/vertex of this square, formed by 1 straight line, parallel OR, and s of straight line, parallel OM. To point T will correspond number $l(p+qi)+s(-q+pi)=lp-sq+(lq+sp)i$, and quotient

of the division of this number into p+qi is equal 1-si. As far as

points are concerned, which lie within any square or on its sides,

but which do not coincide with its apexes/vertexes, then they

represent the numbers, which do not separate into this modulus p+qi.

Let be given any two squares Γ and Δ . Let us superimpose

these squares one on top of the other so that their corresponding

apexes/vertexes would coincide. Let us name the internal points of

these squares, which coincided during this imposition, congruent.

Occurs the very important property which let us formulate in the form

of the following theorem.

Theorem 7.4. The numbers, depicted as congruent points, are

congruent between themselves in modulus/module p+qi.

For simplicity let us take as one of the squares square ORLM

whose apex/vertex O coincides since the origin of the coordinates.

The second square we will propose by such that its apex/vertex Γ,

which corresponds during the imposition to point O, represents number

$(1p-sp)+(1q+sp)i$.

Let certain internal point W of square ORLM represent number

$\dot{A}=a+bi$. Then congruent as it point will represent number

$\dot{B}=(1q-sq+a)+(1q+sp+b)i$. However, the difference $\dot{B}-\dot{A}=(1p-sq)+(1q+sp)$ of

i, as shown above, is divided into p+qi. consequently, $\dot{B} \equiv \dot{A}$ (mod p+qi).

So that the theorem would be proved for any pair of congruent points, it is possible each of the squares to compare with square ORLM, and if $\dot{B}$ and $\dot{B}'$ as the representative points of two different squares, each of which is congruent to the point, which represents number $\dot{A}$, then occur the comparisons

$$\dot{B} \equiv \dot{A} \pmod{p+qi},$$
$$\dot{B}' \equiv \dot{A} \pmod{p+qi},$$

whence it follows that $\dot{B} \equiv \dot{B}'$ (mod p+qi).

Page 395.

From this theorem it is easy to do the following conclusion: in all the incomparable between themselves numbers it can be as much, as integer points are located within any square and on its two not parallel sides, including one apex/vertex, and all these points determine in the set the full/total/complete system of deductions on this modulus. It is possible to geometrically show, that a quantity of such points is equal N=p²+q² and that, therefore, a quantity of deductions in the full/total/complete system is equal to N. However, this was already by purely arithmetic path established/installed by the fundamental theorems of Gauss both for the moduli/modules with

the mutually simple real and alleged parts and for moduli/modules these whose parts have the common divisor, different from unity.

Special role play 4 squares, that have overall apex/vertex at point O. The points of squares have in the known sense the "smallest" coordinates. Under this is understood the following: G(ξ_1, η_1) — the point of square ORLM and H (ξ_2, η_2) — congruent by it the point of any other square (not having by its peak O). Then has place $|\xi_1| \leqslant |\xi_2|$, $|\eta_1| \leqslant |\eta_2|$.

Logical therefore to select any from these squares, in particular square ORLM as containing the points, which correspond to the smallest deductions and which constitute the full/total/complete system of the smallest deductions. As far as squares are concerned remaining three of this type, then they, as can easily be seen, contain the points, which represent the numbers, associated with the specific above smallest deductions.

Thus, the full/total/complete system of the smallest deductions on modulus/module $\dot{m}=p+qi$ can be obtained geometrically by the construction of square with side $\dfrac{\sqrt{N} = |\ \overline{p^2 - q^2}}{i}$ passing through point O, and by the enumeration of all complex integers, represented by the internal points of this square.

Example. To make table of all smallest deductions on modulus/module $\overset{\bullet}{m}=3+4i$ by geometric construction.

Fig. 7.2 depicts the square, constructed on the side $\sqrt{3^2-4^2}$ 5. Let us enumerate all integer points within the square, beginning to the left and moving over the vertical lines. In all such points

$$-3-3i, \quad -3-4i, \quad -2-2i, \quad -2-3i, \quad -2-4i, \quad -2-5i, \quad -1-i,$$
$$-1-2i, \quad -1-3i, \quad -1-4i, \quad -1-5i, \quad -1-6i, \quad 0, \quad i, \quad 2i, \quad 3i, \quad 4i, \quad 5i, \quad 6i,$$
$$1-2i, \quad 1-3i, \quad 1-4i, \quad 1-5i, \quad 2-3i, \quad 2-4i.$$

Page 396.

Here the smallest deductions are represented only by internal points. On the sides of square it did not prove to be integer points. This is characteristic for moduli/modules with mutually simple p and q. If p and q have common factors, then integer points are contained also on the sides of square.

Let us consider another purely arithmetic method of determining the full/total/complete system of the smallest deductions.

Method of determining the borders. Let $\overset{\bullet}{m}=p+qi$ - preset modulus/module and x+iy - smallest deduction on this modulus/module. Method lies in the fact that first define the boundaries themselves of a change in the real part; within the limits of these borders are

defined the possible values of alleged part. The determination of borders is conducted on the basis of the fact that for the smallest deduction must be satisfied the condition:

$$0 \leqslant \frac{px+qy}{p^2+q^2} < 1,$$
$$0 \leqslant \frac{py-qx}{p^2+q^2} < 1 \quad (7.18)$$

or

$$0 \leqslant px + qy = r < p^2 + q^2,$$
$$0 \leqslant py - qx = r' < p^2 + q^2.$$
$$(7.19)$$

Besides the smallest deductions examined and the methods of the determination of the full/total/complete system of the smallest deductions for us subsequently large role will play the least positive residues which were determined earlier into § 7.1. The determination of the full/total/complete system of the least positive residues can be easily realized by the method of determining the borders. Initial inequalities (7.18) and (7.19) will be rewritten for this purpose in the form

$$-\frac{1}{2} < \frac{px-qy}{p^2-q^2} < \frac{1}{2}, \quad -\frac{1}{2} < \frac{py-qx}{p^2-q^2} < \frac{1}{2} \quad (7.20)$$

or

$$-\frac{1}{2}N < px - qy - r < \frac{1}{2}N,$$
$$-\frac{1}{2}N \quad py - qx \quad r' \quad \frac{1}{2}N. \quad (7.21)$$
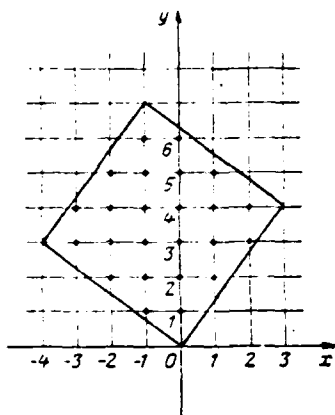
Fig. 7.2. Geometric the representation of the full/total/complete system of the smallest deductions according to modulus/module m=3+4i.

Page 397.

Example. To find the full/total/complete system of the least positive residues from modulus/module $\dot{m} = 3 - 4i$.

Here the system of inequalities (7.21) will take the form

$$-12 \leqslant 3x + 4y = r < 12.$$
$$-12 \leqslant -4x - 3y = r' < 12.$$

For r and r' are possible values of -12, -11,... ,0.1,... ,12. From the given system we obtain the equation

$$25x = 3r - 4r'.$$

Value x will obtain its great positive value with r=+12, r'=-12,

i.e., $25x_{max} \cdot 84$,   whence $x_{max} = 84/25 = 3$. Its respectively small
negative value value x will obtain with r=-12, r'=+12 that gives
x_{min} -3. Thus, for x are possible values of -3, -2, -1, 0,1,2,3. let
us compute the appropriate values of y.

$$1. \quad x = -3 \quad -12 < -9 - 4y < 12, \quad -3 < 4y < 21,$$
$$-12 \leqslant 12 + 3y < 12, \quad -24 < 3y <$$

By testing we establish that these inequalities satisfies only
one value of y=0.

$$2. \quad x = -2; \quad -12 \leqslant -6 + 4y \leqslant 12, \quad -6 < 4y < 18,$$
$$-12 \leqslant 8 + 3y \leqslant 12, \quad -20 \leqslant 3y < 4.$$

From these inequalities we obtain: y=-1, y=0, y=1.

$$3. \quad x = -1 \quad -12 \leqslant -3 + 4y \leqslant 12, \quad -9 \leqslant 4y < 15,$$
$$-12 \leqslant 4 - 3y \leqslant 12, \quad -16 \leqslant 3y \leqslant 8.$$

For y are obtained the values: y=-2, y=-1, y=0, y=1, y=2.

$$4. \quad x = 0 \quad -12 \leqslant 4y \leqslant 12,$$
$$-12 \leqslant 3y \leqslant 12.$$

We obtain for y value: y=-3, y=-2, y=-1, y=0, y=1, y=2, y=3.

$$5. \quad x = 1 \quad -12 \leqslant 3 + 4y \leqslant 12, \quad -15 < 4y < 9,$$
$$-12 \leqslant -4 + 3y \leqslant 12, \quad -8 \leqslant 3y < 16.$$

For y are obtained the values: y=-2, y=-1, y=0, y=1, y=2.

$$6. \quad x = 2. \quad -12 < 6 - 4y \leqslant 12; \quad -18 < 4y < 0,$$
$$-12 < -8 + 3y \leqslant 12; \quad -4 < 3y < 20.$$

We obtain the possible values: y=-1, y=0; y=1.

$$7. \quad x = 3 \quad -12 \leqslant 9 \cdot 4y < 12; \quad -21 < 4y < 3,$$
$$-12 < -12 \cdot 3y < 12; \quad 0 < 3y \leqslant 24.$$

For y is obtained the value: y=0.

In all it is obtained also N=25 values of the least positive residues.

Page 398.

Let us now move on to the geometric interpretation of the full/total/complete system of the least positive residues. Let modulus/module m=p+qi. Let us turn to Fig. 7.1. Let us write the coordinates of the apexes/vertexes of square ORLM: O(o, o), R(-q, p), L(p - q, p+q), M(p, q).

Let us write the equations of straight lines whose intersection formed the square:

(1) прямая $O.M$: $py - qx = 0$,
(1) прямая OR: $px - qy = 0$,
(1) прямая RL: $py - qx = N$,   (7.22)
(1) прямая $L.M$: $px - qy = N$.

Key: (1). straight line.

Comparing these equations with (7.19), we see that they reflect limitations in those permitted of a change in values x and

y-component of the least positive residues they compile an equation

of straight lines by intersection of which is formed the square,

which contains the internal points, which correspond to the

full/total/complete system of the least positive residues in the

following form:

$$py - qx = -\frac{N}{2}, \quad py - qx = \frac{N}{2},$$

$$px + qy = -\frac{N}{2}, \quad px + qy = \frac{N}{2}. \qquad (7.23)$$

Fig. 7.3 depicts the square, limited by the sides whose

equations are represented (7.23). Here the apexes/vertexes of square

have the following coordinates

$$R\left(\frac{p+q}{2} : -\frac{p-q}{2}\right), \quad Q\left(\frac{p-q}{2} : \frac{p+q}{2}\right),$$

$$J\cdot\left(-\frac{p-q}{2} : \frac{p-q}{2}\right), \quad N\left(-\frac{p-q}{2} : -\frac{p-q}{2}\right).$$

Let us give the geometric interpretation of the theorem of

Gauss.

Page 399.

Earlier it was shown that all numbers a+bi, which separate into

the preset complex number ṁ=p+qi, divide/mark off infinite plane into

many squares with the side, equal to $\sqrt{p^2 - q^2}$. To each number, which

does not separate into modulus/module m=p+qi, corresponds the point,

arranged/located within one of such squares.

All numbers within certain specific square together with zero form the full/total/complete system of deductions. Consequently, there is an infinite multitude of full/total/complete systems of deductions.

The full/total/complete system of the smallest deductions contains only square ORLM. Further, it is known that the numbers, congruent in modulus/module m, occupy in their squares congruent positions. Let us select among many squares the squares which contain real deductions from 0 to N-1. On our drawing this will be squares OMN_1N_2; $N_1MN_3N_4$; $N_1N_4N_5N_6$; $N_4N_7N_8N_5$ (see Fig. 7.1).

Among these squares, obviously, there are no such which are congruent relative to real axis. In fact, by hypothesis $(p,q) = 1$ therefore first in the natural series real number, which separates into modulus/module $\dot{m}=p+qi$, will be number p^2+q^2 (in Fig. 7.1 apex/vertex of square N_8), therefore, only beginning from square $N_8N_9N_{10}N_{11}$ it begins the repetition of the squares indicated, and this it means that for all real deductions from the squares indicated will be located the congruent points squared ORLM of the full/total/complete system of the smallest deductions.

MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU

Fig. 7.3. Geometric representation of the full/total/complete system of absolute-smallest deductions according to modulus/module m=p+qi.

Page 400.

§ 7.4. Primitive roots and indices.

Theorem 7.5. If a+bi - complex integer, mutually simple with the prime number $\dot{m}$=p+qi whose norm is equal to N=p²+q², then

$$(a + bi)^{N-1} \equiv 1 \pmod{\dot{m}}.$$

Proof. Let A indicate the set of the full/total/complete system of deductions $\dot{\alpha}, \dot{\beta}, \dot{\gamma},.$ on modulus/module $\dot{m}$, from which is rejected/thrown out zero deduction.

We form products $(a+bi)\dot{\alpha}, (a+bi)\dot{\beta}, (a+bi)\dot{\gamma},....,$ set of which let us

designate through A'.

these products is divisible by $\dot{m}$ and therefore lack of
It is obvious, none of them has the congruent with it deduction

in set A, i.e., $(a+bi)\dot{\alpha} \equiv \dot{\alpha}'(\mathrm{mod}\,\dot{m})$, $(a+bi)\dot{\beta} \equiv \dot{\beta}'(\mathrm{mod}\,\dot{m})$, $(a+bi)\cdot\dot{\gamma} \equiv \dot{\gamma}'(\mathrm{mod}\,\dot{m})$, ...,

where $\dot{\alpha}', \dot{\beta}', \dot{\gamma}', \ldots$ - number of the set A. The set of numbers

$\dot{\alpha}', \dot{\beta}', \dot{\gamma}', \ldots$ let us designate through A". We further form such

products of numbers in each set A, A', A":

$$\dot{P} = \dot{\alpha}\dot{\beta}\dot{\gamma}\ldots,$$
$$\dot{P}' = (a+bi)^{N-1}\dot{\alpha}\dot{\beta}\dot{\gamma}\ldots = (a+bi)^{N-1}\cdot\dot{P},$$
$$\dot{P}'' = \dot{\alpha}'\cdot\dot{\beta}'\cdot\dot{\gamma}'\ldots$$

But numbers of set A" are consecutively/serially congruent with

numbers of set A' and $\dot{P}' \equiv P''$ (mod $\dot{m}$) (since numbers of set A" coincide

with numbers of set A, undertaken in the changed order); therefore

$\dot{P} \equiv \dot{P}'$ (mod $\dot{m}$) either

$$\dot{P} \equiv (a+bi)^{N-1}\dot{P}\,(\mathrm{mod}\,\dot{m}),$$
$$[(a+bi)^{N-1} - 1]\dot{P} \equiv 0\,(\mathrm{mod}\,\dot{m}),$$

whence, since $\dot{m}$ - prime number does not enter into the single

dividers/denominators of number $\dot{P} = \dot{\alpha}\cdot\dot{\beta}\cdot\dot{\gamma}\ldots$

$$(a+bi)^{N-1} - 1 \equiv 0\,(\mathrm{mod}\,\dot{m})$$

or

QED.

$$(a+bi)^{N-1} \equiv 1\,(\mathrm{mod}\,\dot{m}),$$

Page 401.

Theorem 7.6. If a+bi - complex integer, mutually simple with the simple complex integer $\dot{m}=p+qi$ with the norm, equal to N, and t - smallest index, for which $(a+bi)^t \equiv 1 \pmod{\dot{m}}$, the t is the divider/denominator of any other index k, for which $(a-bi)^k \equiv 1 \pmod{\dot{m}}$.

Proof. Let us assume that t is not divider/denominator k; it is obvious, there is such integer n, for which difference nt-k<t. Further from $(a - bi)^t \equiv 1 \pmod{\dot{m}}$ and $(a+bi)^k \equiv 1 \pmod{\dot{m}}$ follows that

$$(a+bi)^{nt} - (a+bi)^k \equiv \pmod{\dot{m}},$$

whence

$$(a+bi)^k \cdot [(a+bi)^{nt-k} - 1] \equiv 0 \pmod{\dot{m}}$$

or

$$(a+bi)^{nt-k} \equiv 1 \pmod{\dot{m}},$$

i.e. they arrived at the fact that there is a degree of number a+bi with an index less than t, which is congruent with unity. This contradicts assumption.

Corollary. t divides or equally N-1, since according to theorem 7.5

$$(a+bi)^{N-1} \equiv 1 \pmod{\dot{m}}.$$

Determination. Complex integer $\dot{h}$, mutually simple with the simple complex integer $\dot{m}$, with the norm, equal to N, is called

primitive roots on modulus/module $\dot{m}$, if the smallest exponent of number h_{j}, congruent with unity in modulus/module $\dot{m}$, is equal to N-1.

Theorem 7.7. If $\dot{h}$ designates primitive roots on modulus/module $\dot{m}$ whose norm is equal to N, then the terms of series/row 1, $\dot{h}, \dot{h}^2, \ldots, \dot{h}^{N-2}$ will be pair-wise incomparable between themselves, i.e., this series represents the full/total/complete system of deductions, if we to it join zero element/cell.

Page 402.

Proof. Actually/really, from

$$\dot{h}^l \equiv \dot{h}^k \,(\mathrm{mod}\,\dot{m})$$
$$0 \leqslant k < l < p-1$$

it would follow

$$\dot{h}^{l-k} \equiv 1 \,(\mathrm{mod}\,\dot{m})$$
$$0 < l-k < p-1.$$

This contradicts the determination of primitive roots, i.e., to theorem condition, therefore, we have N-1 the incomparable between themselves numbers, which form the full/total/complete system of deductions, with exception of zero deduction.

From theorem 7.7 it follows that for any number $\dot{A}=a+bi$, mutually simple with modulus/module $\dot{m}$, comparison $\dot{h}^x \equiv \dot{A}\,(\mathrm{mod}\,\dot{m})$ has unique

solution μ. As in case of real numbers, let us name μ the index of number $\dot{A}$ on modulus/module $\dot{m}$. By analogy with region of real numbers correctly following:

$$\text{ind}\,[(a+bi)\cdot(c+di)\cdot(k+li)\ldots] \equiv$$
$$\equiv (\text{ind}\,(a+bi) + \text{ind}\,(c+di) + \text{ind}\,(k+li) + \ldots)(\text{mod}\,N-1).$$

Actually we have:

$$a+bi \equiv \dot{h}^{\text{ind}\,(a+bi)}\,(\text{mod}\,\dot{m}),$$
$$c+di \equiv \dot{h}^{\text{ind}\,(c+di)}\,(\text{mod}\,\dot{m}),$$
$$k+li \equiv \dot{h}^{\text{ind}\,(k+li)}\,(\text{mod}\,\dot{m}),$$
$$\ldots \ldots \ldots \ldots \ldots$$

After multiplication we will obtain

$$(a+bi)\cdot(c+di)\cdot(k+li)\ldots \equiv$$
$$\equiv \dot{h}^{\text{ind}\,(a+bi)+\text{ind}\,(c+di)+\text{ind}\,(k+li)+\ldots}\,(\text{mod}\,\dot{m}),$$

on the other hand,

$$(a+bi)\cdot(c+di)\cdot(k+li)\ldots \equiv$$
$$\equiv \dot{h}^{\text{ind}\,[(a+bi)\cdot(c+di)\cdot(k+li)\ldots]}(\text{mod}\,\dot{m}).$$

Analyzing two latter/last expressions, we come to the assertion

$$\text{ind}\,[(a+bi)\cdot(c+di)\cdot(k+li)\ldots] \equiv$$
$$\equiv (\text{ind}\,(a+bi) + \text{ind}\,(c+di) + \text{ind}\,(k+li) + \ldots)(\text{mod}\,N-1).$$

Page 403.

Example. Let us construct table of indices for the modulus/module $5+2i$. Here as the primitive roots, i.e., for the basis of index it is possible to take 2, since $2^{2t} \equiv 1\,(\text{mod}\,5-2i)$. We find:

$$2^0 \equiv 1 \qquad 2^{10} \equiv -3+i \qquad 2^{20} \equiv -1+2i$$
$$2^1 \equiv 2 \qquad 2^{11} \equiv 1-i \qquad 2^{21} \equiv -i$$
$$2^2 \equiv -1-2i \qquad 2^{12} \equiv 2-2i \qquad 2^{22} \equiv -2+2i$$
$$2^3 \equiv 1+3i \qquad 2^{13} \equiv 2+i \qquad 2^{23} \equiv -2+i$$
$$2^4 \equiv -1-i \qquad 2^{14} \equiv -1 \qquad 2^{24} \equiv 3-i$$
$$2^5 \equiv -2-2i \qquad 2^{15} \equiv -2 \qquad 2^{25} \equiv -1+i$$
$$2^6 \equiv 1-2i \qquad 2^{16} \equiv 1+2i \qquad 2^{26} \equiv -2+2i$$
$$2^7 \equiv i \qquad 2^{17} \equiv -1-3i \qquad 2^{27} \equiv -2-i$$
$$2^8 \equiv 2i \qquad 2^{18} \equiv 1+i$$
$$2^9 \equiv 2-i \qquad 2^{19} \equiv 2+2i$$

Therefore table will be represented in the following form:

$$\dot{m} = 5+2i; \quad N = 29; \quad h = 2.$$

Ин-декс (1)	Вычет (2)	Ин-декс (1)	Вычет (2)	Ин-декс (1)	Вычет (2)	Ин-декс (1)	Вычет (2)
0	1	8	$2i$	15	-2	22	$-2+2i$
1	2	9	$2-i$	16	$1+2i$	23	$-2+i$
2	$-1-2i$	10	$-3+i$	17	$-1-3i$	24	$3-i$
3	$1+3i$	11	$1-i$	18	$1+i$	25	$-1+i$
4	$-1-i$	12	$2-2i$	19	$2+2i$	26	$-2+2i$
5	$-2-2i$	13	$2+i$	20	$-1+2i$	27	$-2-i$
6	$1-2i$	14	-1	21	$-i$		
7	i						

Key: (1). Index. (2). Deduction.

§ 7.5. System of residual classes in complex domain.

In the present paragraph by analogy with real region we will construct the system of residual classes for complex integers.

Let us select n of mutually prime complex numbers $\dot{m}_1$, $\dot{m}_2, \ldots, \dot{m}_i, \ldots, \dot{m}_n$ by the basis of system $\dot{M}$ and $\dot{M} = \dot{m}_1 \cdot \dot{m}_2 \cdots, \dot{m}_n$.

Page 404.

Let us name complex number $\dot{A}=a+bi$ representable in this system $\dot{M}$, if $a+bi$ it is the smallest deduction on modulus/module $\dot{M}$, otherwise of $\dot{A}$ it is not represented in this system. Since norm $\dot{M}$ is equal to the product of norms $\dot{m}_j$, and a quantity of the smallest deductions is equal to norm $\dot{M}$, the total quantity of representable numbers is equal to the product of the norms of bases/bases.

Let us designate the smallest composite deductions of number $\dot{A}$ on bases/bases $\dot{m}_1, \dot{m}_2, \ldots, \dot{m}_n$ respectively through $\dot{\alpha}_1, \dot{\alpha}_2, \ldots, \dot{\alpha}_{n-1}$

Theorem 7.8. In the system with mutually simple bases/bases $\dot{m}_1, \dot{m}_2, \ldots, \dot{m}_n$ any represented number $\dot{A}=a+bi$ the only form is represented as the set of its smallest deductions on the basis of the system: $(\dot{\alpha}_1, \dot{\alpha}_2, \ldots, \dot{\alpha}_n)$.

Proof. According to the determination of values $\dot{\alpha}_1, \dot{\alpha}_2, \ldots, \dot{\alpha}_n$ take the place of the comparison:

$$\dot{A} \equiv \dot{\alpha}_1 \,(\text{mod}\,\dot{m}_1),$$

$$\dot{A} \equiv \dot{\alpha}_2 \,(\text{mod}\,\dot{m}_2), \qquad\qquad (7.24)$$

$$\cdots\cdots\cdots$$

$$\dot{A} \equiv \dot{\alpha}_n \,(\text{mod}\,\dot{m}_n).$$

Let us assume that there is one additional represented number $\dot{A}'$, represented as the same set of the smallest deductions. Then for it are valid the same comparisons

$$\dot{A}' \equiv \dot{\alpha}_1 \,(\text{mod}\,\dot{m}_1),$$

$$\dot{A}' \equiv \dot{\alpha}_2 \,(\text{mod}\,\dot{m}_2),$$

$$\cdots\cdots\cdots$$

$$\dot{A}' \equiv \dot{\alpha}_n \,(\text{mod}\,\dot{m}_n).$$

Page 405.

Hence it follows that must be implemented the comparisons:

$$\dot{A}' \equiv \dot{A} \,(\text{mod}\,\dot{m}_1),$$

$$\dot{A}' \equiv \dot{A} \,(\text{mod}\,\dot{m}_2),$$

$$\cdots\cdots\cdots$$

$$\dot{A}' \equiv \dot{A} \,(\text{mod}\,\dot{m}_n).$$

Then in view of the mutual simplicity of bases/bases $\dot{A}' = \dot{A} \,(\text{mod}\,\dot{M})$.

We assumed that $\dot{A}$ and $\dot{A}'$ - represented numbers. All elements/cells of the class of the smallest deductions are not comparable between themselves, therefore, $\dot{A}$ and $\dot{A}'$ as the congruent

between themselves elements/cells of this class identically coincide.

Thus, represented number $\dot{A}$ is represented in the form
$\dot{A}=(\dot{\alpha}_1, \dot{\alpha}_2, \ldots, \dot{\alpha}_n)$. Let us assume that $\dot{A}$ is represented as another set of
smallest deductions $\dot{A}=(\dot{\beta}_1, \dot{\beta}_2, \ldots, \dot{\beta}_n)$.   This means that are implemented
the comparisons:

$$\dot{A} \equiv \dot{\beta}_1 \,(\mathrm{mod}\,\dot{m}_1),$$
$$\dot{A} \equiv \dot{\beta}_2 \,(\mathrm{mod}\,\dot{m}_2), \qquad (7.25)$$
$$\cdots\cdots\cdots$$
$$\dot{A} \equiv \dot{\beta}_n \,(\mathrm{mod}\,\dot{m}_n).$$

Comparing (7.24) with (7.25), we obtain the comparisons

$$\dot{\alpha}_1 \equiv \dot{\beta}_1 \,(\mathrm{mod}\,\dot{m}_1),$$
$$\dot{\alpha}_2 \equiv \dot{\beta}_2 \,(\mathrm{mod}\,\dot{m}_2),$$
$$\cdots\cdots\cdots$$
$$\dot{\alpha}_n \equiv \dot{\beta}_n \,(\mathrm{mod}\,\dot{m}_n),$$

whence for reasons presented above follows $\dot{\alpha}_1 = \dot{\beta}_1$, $\dot{\alpha}_2 = \dot{\beta}_2$, $\ldots$, $\dot{\alpha}_n = \dot{\beta}_n$.
Deductions $\dot{\alpha}_1, \dot{\alpha}_2, \ldots, \dot{\alpha}_n$ we will call the digits of the representation
of a number in this system.

Let us give an example of the representation of numbers in the system
of the residual classes

$$\dot{m}_1 = 2+3i, \quad \dot{m}_2 = 3+4i, \quad \dot{m}_3 = 1+4i, \quad \dot{M} = -74-7i.$$

Norm N=5525.

Page 406.

Example. To show that number $\dot{A}=-56-78i$ is represented number and to write its image in the adopted system. It is necessary to show that $\dot{A}=-56-78i$ - the smallest deduction on the modulus/module - 74-7i.

According to formula (7.5) we obtain x=-56 and y=-78. From the same formula let us find the digits of number $\dot{A}$

$$\dot{\alpha}_1 = 2+3i; \ \dot{\alpha}_2 = 5i; \ \dot{\alpha}_3 = -2+2i.$$

Thus $\dot{A} = -56+78i = (-2+3i; \ 5i; \ -2+2i).$

Above is introduced the system of residual classes for complex numbers, taking as the digits of the representation of number $\dot{A}$ the smallest deductions $\dot{A}$ according to the basis of system. Analogously can be constructed the system of residual classes, if we as the digits of the representation of number $\dot{A}$ take its least positive residues. From the point of view of the real system of residual classes this path is equivalent to the use/application both of positive and negative digits α_i on real basis/base p_i with the fact, in order to $|\alpha_i| < \frac{p_i}{2}$. For complex domain the possibility of the construction of system with the least positive residues as the digits has very important value in view of the special features/peculiarities in the location of the represented numbers in the overall range, inherent in this method of representation. For the representation by means of absolutely the smallest deductions occurs

the theorem, analogous to theorem 7.8 about the uniqueness of the
image of the represented number in the system with the mutually
simple bases/bases. In this case it goes without saying the
represented number is defined as belonging to the class of the least
positive residues on modulus/module $\overset{\bullet}{M}$.

A theoretically important question is the
production/consumption/generation of the sign/criterion by which it
is possible to judge about the equipment of this number with the set
of $\overset{\bullet}{M}$, described by the chosen bases/bases. If in the real
region this question is solved simply: number $A \in \mathscr{P}$ when and only
when $A < \mathscr{P}$, where $\mathscr{P}$ - product of real bases/bases, then in the
composite plane the corresponding criterion is expressed by the
system of the inequalities whose practical use is complicated.

Page 407.

In particular, so that the preset number $\overset{\bullet}{A}=a+bi$ would be
represented in system $\overset{\bullet}{M}=p+qi$ of the smallest deductions, it is
necessary and sufficient so that would be satisfied the condition

$$0 \leqslant ap + bq = r < p^2 + q^2 = N,$$
$$0 < bp - aq \quad r' < p^2 + q^2 = N. \qquad (7.26)$$

Let us find now the conditions, superimposed on components of
the complex number $\overset{\bullet}{A}=a+bi$, represented in system $\overset{\bullet}{M}$.

Theorem 7.9. If $\dot{A}=a+bi$, it is represented in system $\dot{M}=p+qi$ of the smallest deductions, then for components a and b has the place:

a) $-q<a<p,\ 0\leqslant b<p+q$ (1при $p>0,\ q>0$;

b) $0\leqslant a<p-q,\ q<b<p$ (1при $p>0,\ q<0$;

c) $p-q<a\leqslant 0,\ p<b<q$ (1при $p<0,\ q>0$;

d) $p<a<-q,\ p-q<b<0$ (1при $p<0,\ q<0$.

Key: (1). with.

Proof. Let $\dot{A}=1+bi$ be is represented in system $\dot{M}$ of the smallest deductions, then from (7.26) it follows

$$a=\frac{pr-qr'}{N},\qquad\qquad (7.27)$$

$$b=\frac{qr+pr'}{N},\qquad\qquad (7.28)$$

where $0\leqslant r<N$; $0\leqslant r'<N$.

a) According to condition $p>0$, $q>0$; therefore if we take $r=N$ and $r'=0$ in expression (7.27) and $r=r'=N$ in expression (7.28), then we will obtain

$$a=\frac{pr-qr'}{N}<\frac{p.N}{N}=p.$$

$$b=\frac{qr+pr'}{N}<\frac{q.N-pN}{N}=q+p.$$

i.e. $a<p$, $b<q+p$.

On the other hand, after taking in (7.27) $r=0$, $r'=N$ and in (7.28) $r=r'=0$, we will obtain $a>-q$, $b\geqslant 0$.

b) On condition $p > 0$, $q < 0$; therefore

$$a = \frac{pr - qr'}{N} < \frac{p.N - q.N}{N} = p - q,$$

$$b = \frac{qr + pr'}{N} < \frac{0 \cdot q - p.N}{N} = p.$$

Page 408.

On the other hand,

$$a \geqslant \frac{p \cdot 0 - q \cdot 0}{N} = 0, \quad b > \frac{p \cdot 0 + qN}{N} = q.$$

c) Since $p < 0$, $q > 0$, then

$$a \leqslant \frac{p \cdot 0 - q \cdot 0}{N} = 0, \quad b < \frac{qN - p \cdot 0}{N} = q,$$

$$a > \frac{p \cdot N - qN}{N} = p - q, \quad b > \frac{q \cdot 0 + pN}{N} = p.$$

d) With $p < 0$, $q < 0$

$$a < \frac{p \cdot 0 - qN}{N} = -q, \quad b \leqslant \frac{p \cdot 0 - q \cdot 0}{N} = 0,$$

$$a > \frac{pN - q \cdot 0}{N} = p, \quad b > \frac{qN + pN}{N} = q + p.$$

Determination. Complex integer $\dot{A} = a + bi$ we will call represented in the system of absolutely smallest subtractions, if it is the least positive residue on modulus/module $\dot{M} = p + qi$.

Similar to the system of the smallest deductions it is possible to find necessary and sufficient conditions of the representability of number $\dot{A}$ in system $\dot{M}$ absolutely of the smallest deductions with norm N which are

$$-\frac{N}{2} \leqslant ap + bq = r < \frac{N}{2} ;$$

$$-\frac{N}{2} \leqslant bp - aq = r' \leqslant \frac{N}{2} . \tag{7.29}$$

Theorem 7.10. If $\dot{A} = a - bi$ is represented in system $\dot{M} = p + qi$ of the

least positive residues, then components a and b satisfy the following conditions:

a) $-\frac{1}{2}(p+q) \leqslant a \leqslant \frac{1}{2}(p+q)$, $-\frac{1}{2}(p+q) \leqslant b \leqslant \frac{1}{2}(p+q)$
   (1)при $p>0$, $q>0$;

б) $-\frac{p-q}{2} \leqslant a \leqslant \frac{p-q}{2}$, $-\frac{p-q}{2} \leqslant b \leqslant \frac{p-q}{2}$
   при $p>0$, $q<0$;

в) $\frac{p-q}{2} \leqslant a \leqslant \frac{-p-q}{2}$, $\frac{p-q}{2} \leqslant b \leqslant \frac{-p-q}{2}$
   при $p<0$, $q>0$;

г) $\frac{p+q}{2} \leqslant a \leqslant \frac{-p-q}{2}$, $\frac{p+q}{2} \leqslant b \leqslant \frac{-p-q}{2}$
   при $p<0$, $q<0$.

Key: (1). with.

Page 409.

Proof. Let us suppose $\dot{A}=a+bi$ is represented in system $\dot{a}=p+qi$ absolutely of the smallest deductions, then

$$a = \frac{pr-qr'}{N},\qquad (7.30)$$

$$b = \frac{qr+pr'}{N},\qquad (7.31)$$

where $-\frac{N}{2} \leqslant r \leqslant \frac{N}{2}$; $-\frac{N}{2} \leqslant r' \leqslant \frac{N}{2}$.

a) According to condition p>0, q>0, therefore, if we take in expressions (7.30) and (7.31) respectively

$$r=\frac{N}{2},\ r'=-\frac{N}{2}\ \text{and}\ \ r=\frac{N}{2},\ r'=\frac{N}{2}.$$

then we will obtain upper bounds for a and b

$$a \leqslant \frac{p\frac{N}{2}+q\frac{N}{2}}{N} = \frac{p+q}{2}, \quad b \leqslant \frac{q\frac{N}{2}+p\frac{N}{2}}{N} = \frac{p-q}{2}.$$

For lower boundaries let us place in expressions (7.30) and (7.31) respectively the values:

$$r = -\frac{N}{2}, \quad r' = \frac{N}{2} \quad \overset{(*)}{\text{H}} \quad r = -\frac{N}{2}, \quad r' = -\frac{N}{2}$$

$$a \geqslant \frac{-p\frac{N}{2} - q\frac{N}{2}}{N} = -\frac{p+q}{2}, \quad b \geqslant \frac{-q\frac{N}{2} - p\frac{V}{2}}{N} = -\frac{p-q}{2}.$$

Key: (1). and.

Analogously are proven cases b, c and d.

With the carrying-out of the arithmetic operations of the relationship/ratio between the digits of the representation of the components of operations and result the same as in the real region.

Theorem 7.11. $\dot{A} = (\dot{\alpha}_1, \dot{\alpha}_2, \ldots, \dot{\alpha}_n)$, $\dot{B} = (\dot{\beta}_1, \dot{\beta}_2, \ldots, \dot{\beta}_n)$, $\dot{C} = \dot{A} + \dot{B} = (\dot{\gamma}_1, \dot{\gamma}_2, \ldots, \dot{\gamma}_n)$;

then $\dot{\alpha}_j + \dot{\beta}_j = \dot{\gamma}_j + \dot{\tau}_j \cdot \dot{m}_j$, where $\dot{\tau}_j$ - one of the numbers 0, 1, i, 1+i in first type system and further in second type system.

Page 410.

Proof. $\dot{\alpha}_j = a_1 + b_1 i$, $\dot{\beta}_j = a_2 + b_2 i$. The circumstance that $\dot{\alpha}_j$ and $\dot{\beta}_j$ - digit on basis/base $\dot{m}_j = p_j + q_j i$, indicates for first type systems that:

$$0 \leqslant \frac{b_1 p_j - a_1 q_j}{p_j^2 + q_j^2} < 1, \quad 0 \leqslant \frac{a_1 p_j + b_1 q_j}{p_j^2 + q_j^2} < 1. \quad (7.32)$$

$$0 \leqslant \frac{a_2 p_j + b_2 q_j}{p_j^2 + q_j^2} < 1, \quad 0 \leqslant \frac{b_2 p_j - a_2 q_j}{p_j^2 + q_j^2} < 1.$$

For sum $\dot{\alpha}_j + \dot{\beta}_j$ it is possible to write

$$\frac{\dot{\alpha}_j + \dot{\beta}_j}{p_j + iq_j} = \frac{(a_1 + a_2) p_j + (b_1 + b_2) q_j}{p_j^2 + q_j^2} + \frac{(b_1 + b_2) p_j - (a_1 + a_2) q_j}{p_j^2 + q_j^2} i.$$

$$(7.33)$$

In the comparison (7.32) it is possible to write

$$0 < \frac{(a_1 - a_2)\,p_j + (b_1 - b_2)\,q_j}{p_j^2 + q_j^2} < 2, \quad 0 < \frac{(b_1 - b_2)\,p_j - (a_1 + a_2)\,q_j}{p_j^2 + q_j^2} < 2.$$

(7.34)

i.e. in each of these fractions it is possible to isolate whole part, equal to 0 or 1, whence follows the assertion of theorem.

For second type system occur the inequalities:

$$-\frac{1}{2} < \frac{b_1 p_j - a_1 q_j}{p_j^2 + q_j^2} \leqslant \frac{1}{2}, \quad -\frac{1}{2} < \frac{a_1 p_j + b_1 q_j}{p_j^2 + q_j^2} \leqslant \frac{1}{2}, \quad (7.35)$$

$$-\frac{1}{2} < \frac{a_2 p_j + b_2 p_j}{p_j^2 + q_1^2} \leqslant \frac{1}{2}, \quad -\frac{1}{2} < \frac{b_2 p_j - a_2 q_j}{p_j^2 + q_j^2} \leqslant \frac{1}{2}.$$

Then it is possible to write

$$-1 < \frac{(a_1 + a_2)\,p_j + (b_1 + b_2)\,q_j}{p_j^2 + q_j^2} \leqslant 1,$$

$$-1 < \frac{(b_1 - b_2)\,p_j - (a_1 + a_2)\,q_j}{p_j^2 - q_j^2} \leqslant 1.$$

(7.36)

From these inequalities also follows the assertion of theorem for the representation in second type system.

$\dot{A}(\dot{\alpha}_1, \dot{\alpha}_2, \ldots, \dot{\alpha}_n)$ and $\dot{B}(\dot{\beta}_1, \dot{\beta}_2, \ldots, \dot{\beta}_n)$ - two complex integers, represented in system B, where $\dot{\alpha}_j, \dot{\beta}_j$ - smallest or absolutely the smallest deductions.

Page 411.

Then, if $\dot{A}+-\dot{B}$, $\dot{A}\dot{B}$ are representable in system $\dot{M}$, on the basis of the property of comparisons we have:

$$\dot{A}+\dot{B} = (\dot{\alpha}_1+\dot{\beta}_1;\ \dot{\alpha}_2-\dot{\beta}_2;\ \ldots;\ \dot{\alpha}_n-\dot{p}_n).$$
$$\dot{A}-\dot{B} = (\dot{\alpha}_1-\dot{\beta}_1;\ \dot{\alpha}_2-\dot{\beta}_2;\ \ldots;\ \dot{\alpha}_n-\dot{\beta}_n).$$
$$\dot{A}\cdot\dot{B} = (\dot{\alpha}_1\cdot\dot{\beta}_1;\ \dot{\alpha}_2\cdot\dot{\beta}_2;\ \ldots;\ \dot{\alpha}_n\cdot\dot{\beta}_n).$$

In this case sum $\dot{\alpha}_j+\dot{\beta}_j$, product $\dot{\alpha}_j\cdot\dot{\beta}_j$ and difference $\dot{\alpha}_j-\dot{\beta}_j$ are taken respectively on moduli/modules $\dot{m}_j$.

Example.

a) $\dot{A}=4+5i=(-i,\ -1,\ -2i)$; $\dot{B}=1-4i=(-i,\ \ \ -1,-1-i)$.

Let as system $\dot{M}$ be undertaken

$$\dot{m}_1 = 1+i,\ \dot{m}_2 = 2+i,\ \dot{m}_3 = 3-2i.$$

then $\dot{M}=-3+11i$.

Let us find sum $\dot{A}+\dot{B}=(-i,\ -1,\ -2i)+(-i,\ -1,\ -1-i)=(2i,\ -2,\ -1-3i)$ or into absolutely the smallest deductions $\dot{A}+\dot{B}=(0,\ i,\ 2i)$. Easily it is checked, that a number $(0,\ i,\ 2i)$ exists $5+i$ and it is equal to sum $(4+5i)+(1-4i)$.

b) $\dot{A}=3+5i=(0,\ i,\ 2)$; $\dot{B}=1+4i=(-i,\ i,\ -i)$.

Let us find the difference $\dot{A}-\dot{B}=(i,\ 0,\ 2+i)$ or in least positive residues $\dot{A}-\dot{B}=(i,\ 0,\ -1-i)$. By direct testing we establish that a number $(-i,\ 0,\ -1-i)$ exists $2+i$ and it is equal to difference

(3+5i)-1+4i).

$$\dot{A} = 1 + 3i = (0, 0, -2i); \quad \dot{B} = 1 - i = (0, -i, 1+i).$$

Let us find product $\dot{A}\dot{B}$=(0, 0, 2-2i) or in absolutely the smallest deductions $\dot{A}\dot{B}$=(0, 0, 1). By testing we are convinced, that number (0, 0, i) is actually/really product (1+3i)x(1+i)=-2+4i.

The operations of addition, subtraction and multiplication examined relate to a number of accurately of feasible above any arbitrarily those undertaken numbers; from the point of view of uniqueness it suffices to require the nonappearance of result of operation for the range of the representation of numbers accepted.

However, division feasibly hardly ever. Therefore in the system of residual classes we examine the operation of division only when it can be carried out with obtaining of exact quotient.

Page 412.

However, generally it is possible to examine the case of the division, when quotient is not integer. In this case we obtain formal quotient.

Let $\dot{A} = (\dot{\alpha}_1, \dot{\alpha}_2, \ldots, \dot{\alpha}_n)$ be divided without the remainder/residue into $\dot{B} = (\dot{\beta}_1, \dot{\beta}_2, \ldots, \dot{\beta}_n)$. Let us find the quotient

$$\dot{C} = \frac{\dot{A}}{\dot{B}} = (\dot{\gamma}_1, \dot{\gamma}_2, \dots, \dot{\gamma}_n),$$

whence $\dot{C}\dot{B} = \dot{A}$ and

$$(\dot{\beta}_1\dot{\gamma}_1 - \dot{k}_1\dot{m}_1; \dot{\beta}_2\dot{\gamma}_2 - \dot{k}_2\dot{m}_2, \dots, \dot{\beta}_n\dot{\gamma}_n - \dot{k}_n\dot{m}_n) = (\dot{\alpha}_1, \dot{\alpha}_2, \dots, \dot{\alpha}_n),$$

where $\dot{k}_j$, to eat one of the deductions of full/total/complete system on modulus/module $\dot{m}_j$. From this equality we have

$$\dot{\gamma}_1 = \frac{\dot{\alpha}_1 + \dot{k}_1\dot{m}_1}{\dot{\beta}_1}, \quad \dot{\gamma}_2 = \frac{\dot{\alpha}_2 + \dot{k}_2\dot{m}_2}{\dot{\beta}_2}, \dots, \dot{\gamma}_n = \frac{\dot{\alpha}_n - \dot{k}_n\dot{m}_n}{\dot{\beta}_n},$$

from which it is clear that the components of quotient are obtained by the step-by-step division of the corresponding components of dividend and divider/denominator, in this case if there is no fissionability completely, then to the component of dividend is adjoined the corresponding basis/base, multiplied by this deduction $\dot{k}_j$, so that $\dot{\alpha}_j + \dot{k}_j\dot{m}_j$ would be divided completely into $\dot{\beta}_j$. It is obvious, this division in a single manner will determine digit $\dot{\gamma}_j$, if $\dot{k}_j$ will be undertaken from the full/total/complete system of deductions.

Example. Let us take system $\dot{M}$ in the following form:

$$\dot{m}_1 = 2 + i; \; \dot{m}_2 = 3 + 2i; \; \dot{m}_3 = 4 + i; \; \dot{M} = 9 + 32i.$$

Let us divide in this system $2 + 4i = (-1; 1-i; -1-i)$ into a number $3 + i = (1, -1, -1)$

$$\frac{2+4i}{3+i} = \left(\frac{-1}{1}; \frac{1-i}{-i}; \frac{-1-i}{-1}\right) = (-1; 1+i; 1+i).$$

By testing we are convinced, which $(-1; 1+i; 1+i)$ is quotient of the division $2+4i$ on $3+i$, i.e., $1+i$.

Example. Let us take system $\dot{m}_1 = 1+i$; $\dot{m}_2 = 2+i$; $\dot{m}_3 = 3+2i$; $\dot{M} = -3+11i$.
Let us consider the division of a number 4+4i into a number -4+i with
obtaining of the formal quotient

$$\frac{4-4i}{-4+i} = \frac{(0,\ 1,\ -2)}{(1,\ -1,\ 1)} = (0,\ -1,\ -2) = -1+5i.$$

Page 413.

●

Actually/really, -1+5i there is the formal quotient, obtained, when
as the dividend is taken 4+4i plus product -2+i to the modulus/module
of system -3+11i.

If divider/denominator is divided into any basis/base $\dot{m}_j$, then
this it means that the remainder/residue on this basis/base is equal
to zero, however, since is assumed that the division is implemented
completely, then the corresponding remainder/residue of dividend is
also equal to zero; therefore we have in this case step-by-step
division of 0/0, i.e., uncertainty/indeterminancy. The
disclosure/expansion of this type of uncertainties/indeterminancies
requires the enlistment of further considerations.

The methodology of the translation/conversion of number
$\dot{A}(\dot{\alpha}_1,\ \dot{\alpha}_2,\ \dots,\ \dot{\alpha}_n)$ from the system of residual classes into the positional
system the same as for the real region.

Are chosen the orthogonal bases of the system:

$$\dot{B}_1 = (1, 0, 0, \ldots, 0),$$
$$\dot{B}_2 = (0, 1, 0, \ldots, 0), \qquad (7.37)$$
$$\cdots \cdots \cdots \cdots$$
$$\dot{B}_n = (0, 0, \ldots, 0, 1),$$

such, that

$$\dot{A} \equiv \dot{\alpha}_1\dot{B}_1 + \dot{\alpha}_2\dot{B}_2 + \ldots + \dot{\alpha}_n\dot{B}_n \,(\mathrm{mod}\,\dot{M}). \qquad (7.38)$$

From (7.37) it is evident that

$$\dot{B}_j = \frac{\dot{M}}{m_j}\dot{\psi}_j, \qquad (7.39)$$

moreover $\dot{\psi}_j$, which can be named the weight of composite orthogonal base $\dot{B}_j$ of system $\dot{M}$, is determined from the comparison

$$\frac{\dot{M}}{m_j}\dot{\psi}_j \equiv 1 \,(\mathrm{mod}\,\dot{m}_j). \qquad (7.40)$$

For the clarity let us consider an example of the translation/conversion of the complex number $\dot{A}$.

Example. $\dot{A} = (-1, i, 1+2i)$:

$$\dot{M} = (2+i)\,(3+2i)\,(4+i) = 9 + 32i.$$

Page 414.

Let us construct the orthogonal bases of the system

$$\dot{B}_1 = \frac{9+32i}{2+i}\dot{\psi}_1 \equiv 1 \,(\mathrm{mod}\,2+i) \quad \text{OR} \quad (11-10i)\dot{\psi}_1 \equiv 1 \,(\mathrm{mod}\,2+i).$$

Here $\dot{\psi}_1 = 1$, since $11 - 10i \equiv 1\,(\mathrm{mod}\,2+i)$. Consequently, $\dot{B}_1 = 11 - 10i$,

$$\dot{B}_2 = \frac{9+32i}{3+2i}\dot{\psi}_2 \equiv 1 \,(\mathrm{mod}\,3+2i) \quad \text{OR} \quad (7+6i)\dot{\psi}_2 \equiv 1 \,(\mathrm{mod}\,3+2i).$$

$\dot{\psi}_2 = \dot{x} + iy$; then

$$(7 + 6i)\dot{\psi}_2 = (7x - 6y) + (6x + 7y)i.$$

Through formulas (7.3) we find x and y

$$\begin{aligned} 3(7x - 6y) + 2(6x + 7y) = 3 \\ 3(6x + 7y) - 2(7x - 6y) = -2 \end{aligned} \left. \right\} \begin{aligned} x = 1, \\ y = 1, \end{aligned}$$

therefore $\dot{B}_2 = (7 + 6i)(1 + i) = 1 + 13i,$

$$\dot{B}_3 = \frac{9 + 32i}{4 + i}\dot{\psi}_3 = (4 + 7i)\dot{\psi}_3 \equiv 1 \,(\text{mod } 4 + i).$$

If $\dot{\psi}_3 = x + iy,$ that we obtain $(4x - 7y) + (7x + 4y)i \equiv 1 \,(\text{mod } 4 + i)$. We pass from this composite comparison to the real equalities according to (7.3)

$$\begin{aligned} 4(4x - 7y) + (7x + 4y) = 4 \\ 4(7x + 4y) - (4x - 7y) = -1 \end{aligned} \left. \right\}.$$

Whence x=-1, y-1 and $\dot{B}_3 = -11 - 3i$.

Thus, is found the system of orthogonal bases. Let us register number $\dot{A}$ in the form (7.38)

$$\dot{A} \equiv -1(11 - 10i) + i(1 + 13i) + (1 + 2i)(-11 - 3i) \,(\text{mod } 9 + 32i)$$

or

$$\dot{A} \equiv -29 - 14i \,(\text{mod } 9 + 32i).$$

Absolutely - the smallest deduction of a number -29-14i on the modulus/module 9+32i - number $\dot{A}$ exists 12+9i.

§7.6. On the imbedied systems of the smallest deductions.

In complex domain complex integer a+bi, represented in the

system of the smallest deductions $\dot{M}$, is not always represented in

system $\dot{M}'$, where $N_{\dot{M}'} > N_{\dot{M}'}$ although in system M' of the smallest

deductions a quantity of represented numbers increases.

Page 415.

For the real region this it goes without saying it is impossible,

since the growth of bases/bases leads only to an increase in the

quantity of represented numbers with the

retention/preservation/maintaining of the representability of the

numbers, which entered into the unexpanded range. Analogous property

possesses the system of residual classes with the digits - absolutely

smallest bases/bases, which makes this system of of more preferable

for the realization.

Determination. System $\dot{M}$ of the smallest deductions it will

consider imbedded in system $\dot{M}'$ of the smallest deductions where

$N_{\dot{M}'} > N_{\dot{M}'}$ if any represented in system $\dot{M}$ a number is represented also

in system $\dot{M}'$.

From the geometric interpretation of the system of residual

classes in complex domain it is evident that system $\dot{M}$ - square T

(Fig. 7.4) is imbedded in system $\dot{M}'$ - square G, when the entire set

of the points, which are the smallest deductions of $\dot{M}$,   , is

contained squared G. For system $\dot{M}' = \dot{M}m$ of the smallest deductions $\dot{m}$
(let us note that $\dot{m} \neq 1+i$) must be chosen from the fact that on the
inclination/slope of the straight line OM' is superimposed the
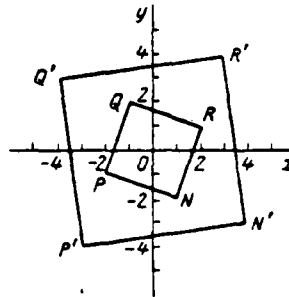specified condition.
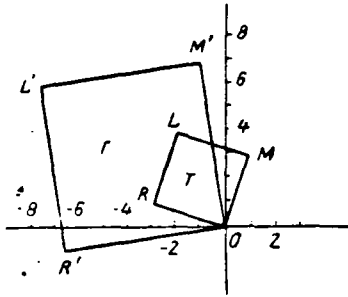
Fig. 7.4.   Fig. 7.5.

Fig. 7.4. Geometric representation of two systems of smallest deductions, one of which M is not imbedded in system M'.

Fig. 7.5. Geometric representation of two systems absolutely of smallest deductions where system M is imbedded in system M'.

Page 416.

System M of the least positive residues is always imbedded in system M'=Mm. Actually/really, square RQPN of system M=p+qi will always prove to be imbedded in square R'Q'P'N' of system M'=(p+qi)(p'+q'i) (Fig. 7.5), since both they originate by center of coordinates, and a radius of the field, circumscribed around square RQPN $\left(R=\frac{1}{2}\sqrt{2(p^2+q^2)}\right)$, is always lower than the radius of field, inscribed into square R'Q'P'N' $\left(R'=\frac{1}{2}\sqrt{(p'^2+q'^2)(p^2+q^2)}\right)$.

Example. $\dot{M}=1+3i$ - system of the smallest deductions.

$$\dot{m}=2+i; \quad \dot{M}'=\dot{M}\dot{m}=-1+7i.$$

From Fig. 7.4 it is evident that system $\dot{M}$ of the smallest deductions is not imbedded in system $\dot{M}'$, since the part of it of the smallest deductions, namely i; 2i; 3i, is not the smallest deductions of system $\dot{M}'$. But if system $\dot{M}=1+3i$ is the system of the least positive residues, then it is imbedded in system $\dot{M}'=-1+7i$ (Fig. 7.5).

§7.7. Isomorphism of systems $\dot{M}$ of composite and real deductions.

Let as the basis of system $\dot{M}$ be undertaken
$$\dot{m}_1=p_1+q_1 i; \quad \dot{m}_2=p_2+q_2 i, \ldots, \dot{m}_n=p_n+q_n i;$$
$$\dot{M}=\dot{m}_1\dot{m}_2\ldots\dot{m}_n=p+qi,$$
with the norms, equal to respectively $N_1, N_2, \ldots N_n, N$, where $(p_j, q_j)=1; (p, q)=1$.

Let be further for each basis/base determined the coefficients of isomorphism $\rho_j=u_j q_j-v_j p_j, \rho=uq-vp$, where u_j, v_j and u, v satisfy conditions of mutual simplicity of numbers p_j, q_j, p, q. i.e.
$$u_j p_j+v_j q_j=1, \quad up+vq=1.$$

Then is valid the following theorem.

Theorem 7.12. Any complex integer $\dot{A}=a+bi$ from the set of

represented in this system numbers is represented in this system in the form $\dot{A} = a + bi = (h_1, h_2, \ldots, h_n)$, where h_j is the least non-negative residue of numbers $a + \rho_j b$ on moduli/modules N_j.

Page 417.

Proof. Proof escape/ensues directly from the theorem of Gauss. Actually/really, since according to condition $(\dot{p}_j, q_j) = 1$, then according to the theorem of Gauss for any number $\dot{A}$ has place $\dot{A} \equiv h_j (\text{mod} \, \dot{m}_j)$, where h_j – the least non-negative residue of number $a - \rho_j b$ on modulus/module N_j; on the other hand, if $\dot{\alpha}_j$ is composite deductions of number $\dot{A}$ respectively on moduli/modules $\dot{m}_j$, then $\dot{A} \equiv \dot{\alpha}_j (\text{mod} \, \dot{m}_j)$, therefore $\dot{\alpha}_j \equiv h_j (\text{mod} \, \dot{m}_j)$, whence in the limits of the representability of a number we have

$$\dot{A} = (\dot{\alpha}_1, \dot{\alpha}_2, \ldots, \dot{\alpha}_n) = (h_1, h_2, \ldots, h_n). \qquad (7.41)$$

Thus, any number of the set of the represented numbers is represented as the sequence of its real deductions on moduli/modules $\dot{m}_j$, i.e.

$$\dot{A} = (h_1, h_2, \ldots, h_n). \qquad (7.42)$$

This means that, representing a number in the form (7.42), we pass from system $\dot{m}$ with bases/bases $\dot{m}_1, \dot{m}_2, \ldots, \dot{m}_n$ to system m with the bases/bases, equal to norms $N_1, N_2, \ldots, N_n$ of these bases/bases, since real deductions h_j are found from the conditions

$$a + b\rho_j \equiv h_j \, (\text{mod} \, N_j),$$

where a and b - components of number $\dot{A}$.

Determination. System M with the bases/bases, equal to norms $N_1, N_2, \ldots, N_n$, we will call system M of real deductions.

It is possible at the necessary moment/torque to always pass from system $\dot{M}$ of composite deductions to system M of real deductions. In this consists the isomorphism of the systems of complex and real deductions.

Further, naturally, arises the question about the existence of system $\dot{M}$, which satisfies conditions of theorem 7.12 about the isomorphism. Let us show that this system exists.

Page 418.

Let $\dot{m}_1 = p_1 - q_1 i; \ \dot{m}_2 = p_2 - q_2 i; \ \ldots \ \dot{m}_n = p_n + q_n i$ be pair-wise mutually prime numbers with norms $N_1, N_2, \ldots, N_n$ and $\dot{M} = \dot{m}_1 \cdot \dot{m}_2 \ldots \dot{m}_n = p + qi$, then, obviously, $(p_j, q_j) = 1$ and $(p, q) = 1$. In fact, since $\dot{m}_j$ - prime

numbers, then according to the sign/criterion of prime numbers their norms must be the prime numbers of form 4k+1. But from the theory of numbers it is known that idle time a number of form 4k+1 is represented in the form of the sum of the squares of two mutually prime numbers; therefore from $N_j = p_j^2 + q_j^2$ it follows that $(p_j, q_j) = 1$.

It is easy to show that the norm of $\dot{M}$ is equal to the product of the norms of cofactors, therefore, it contains only the simple dividers/denominators of form 4k+1 and itself is a number of form 4k+1. Therefore from the criterion of the representability of a number of form 4k+1 by form of $p^2 + q^2$ we consist that $(p, q) = 1$. QED.

The case in question assumes that among the basis of system $\dot{M}$ there are no numbers 1+i with the norm, equal to 2, meanwhile the presence of this basis/base would considerably facilitate the organization of the work on the relative numbers. Therefore let us show that also in the presence of basis/base 1+i in the system occurs mutual simplicity of numbers p and q.

System $\dot{M} = p + qi = \dot{m}_2, \dot{m}_3 \ldots \dot{m}_n$, where $\dot{m}_j$ - pair-wise mutually prime numbers with the norms of form 4k+1, in this case, as shown above, $(p, q) = 1$.

Let us now supplement into this system basis/base $\dot{m}_1 = 1 + i$, i.e.

$\dot{M}' = \dot{M}(1+i) = \dot{m}_1 \dot{m}_2 \ldots \dot{m}_n = (p+qi)(1+i) = p-q) + (p+q)i$. Let us show that p-q and p+q is mutually simple.

Actually/really, the norm of $\dot{M}$ is equal to $N = p^2 + q^2$, however, since number N has dividers/denominators only of form 4k+1, the very number N of also the same form; therefore in its expansion p and q they must be different parity, whence we consist that number p-q and p+q both odd.

Let p-q and p+q have the common divisor, different from 1, i.e., (p-q, p+q)=d, then

$$p - q \equiv 0 \pmod{d}, \quad p + q \equiv 0 \pmod{d}$$

or

$$2p \equiv 0 \pmod{d}, \quad 2q \equiv 0 \pmod{d}.$$

Page 419.

So   p-q and p+q odd, the d - odd divider/denominator; therefore (d, 2) =1, therefore, after reduction to 2 we will obtain

$$p \equiv 0 \pmod{d}, \quad q \equiv 0 \pmod{d}$$

or

$$(p, q) = d > 1,$$

which contradicts the condition of mutual simplicity of numbers p, q. Consequently, p-q and p+q is mutually simple, QED.

Example. $\dot{m}_1 = 1+i$, $\dot{m}_2 = 2+i$, $\dot{m}_3 3+2i$, $\dot{m}_4 = 4+i$, $\dot{m}_5 = 5+2i$, $\dot{m}_6 = 6+i$, $\dot{m}_7 = 5+4i$, $\dot{m}_8 = 2+7i$, $\dot{m}_9 = 6+5i$, $\dot{m}_{10} = 3+8i$. From the norm it is respectively equal to: $N_1 = 2$, $N_2 = 5$, $N_3 = 13$, $N_4 = 17$, $N_5 = 29$, $N_6 = 37$, $N_7 = 41$, $N_8 = 53$, $N_9 = 61$, $N_{10} = 73$, $\dot{M} = 4422219 + 2265865i$.

It is not difficult to check with the help of the euclidean algorithm that numbers 4422219 and 2265865 are mutually simple.

It is obvious, the rules of the arithmetic operations on the complex numbers, represented in the form (7.42), do not differ from the rules of arithmetic operations in the system of residual classes in the real region; therefore special on them we stop will not be.

Let us consider examples. Let us select system $\dot{M}$ in the form:
$\dot{m}_1 = 1+i$, $\dot{m}_2 = 2+1$, $\dot{m}_3 = 3+2i$,

$$\dot{M} = (1+i)(2+i)(3+2i) = -3+11i, \quad N_1 = 2, \quad N_2 = 5,$$

$N_3 = 13$, $N = 130$, and let us determine for this system $\rho_1 = 2 \cdot 1 + 1 \cdot 1 = 3$, $\rho_2 = 1 \cdot 1 + 2 \cdot 1 = 3$, $\rho_3 = 2 \cdot 1 + 3 \cdot 1 = 5$.

Example. Let us register numbers $\dot{A} = -3+4i$ and $\dot{B} = -1-3i$ in the form (7.42). For $\dot{A}$ we have

$$-3 + 4 \cdot 1 \equiv h_1 \pmod{2}, \quad h_1 = 1.$$
$$-3 + 4 \cdot 3 \equiv h_2 \pmod{5}, \quad h_2 = 4.$$
$$-3 + 4 \cdot 5 \equiv h_3 \pmod{13}, \quad h_3 = 4.$$

Therefore $-3+4i = (1, 4, 4)$. For $\dot{B}$ we have:

$$-1 - 3 \cdot 1 \equiv h_1 \pmod{2}, \quad h_1 = 0.$$
$$-1 - 3 \cdot 3 \equiv h_2 \pmod{5}, \quad h_2 = 0.$$
$$-1 - 3 \cdot 5 \equiv h_3 \pmod{13}, \quad h_3 = 10.$$

Therefore $-1-3i = (0, 0, 10)$.

Example. a) To find the sum of numbers $\overset{\bullet}{A} = -3+4i = (1, 4, 4)$ and $\overset{\bullet}{B} = -3-3i = (0, 0, 10)$.

Page 420.

Solution: $(-3+4i)+(-1-3I) = -4+i(1, 4, 4)+(0, 0, 10) = (1, 4, 1)$.

Actually/really, by testing we are convinced, that the sum $-4+i$ is

represented in system $\overset{\bullet}{M}$ in the form $(1, 4, 1)$.

$$\text{b\&)} \quad \dot{A} = 3 = (1, 3, 3), \quad \dot{B} = -1-2i = (1, 3, 4),$$
$$\dot{A} \cdot \dot{B} = (1, 3, 3) \cdot (1, 3, 4) = (1, 4, 12).$$

It is easy to check that number $(1, 4, 12)$ represents product

$\overset{\bullet}{A} \cdot \overset{\bullet}{B} = -3-6i$.

Example. System $\overset{\bullet}{M}$ the same as in the previous example:

$$\dot{A} = 8+6i = (0, 1, 12), \quad \dot{B} = 4+3i = (1, 3, 6),$$
$$\dot{C} = \frac{\dot{A}}{\dot{B}} = \frac{(0, 1, 12)}{(1, 3, 6)} = \left(\frac{0}{1}, \frac{1+1 \cdot 5}{3}, \frac{12}{6} \right) = (0, 2, 2),$$

i.e. quotient $8+6i/4+3i$ is equal $2 = (0, 2, 2)$.

§7.8. Determination of the set of the represented numbers for systems

M of composite deductions with the help of the real deductions.

Let us assume that number x+iy is complex (smallest or absolutely smallest) remainder of number A=a+bi according to modulus M=p+qi, where (p, q)=1.

Then regarding x+iy it is represented in system M of composite deductions. And if h - real deduction of number A on modulus/module M, then has place x+iy=h(modM). If we find composite deductions for numbers h=0, 1, 2, ..., N-1 from modulus/module M, then we will obtain entire set of the represented numbers in system M of composite deductions.

This method is interesting to those that immediately is established a correspondence between the sequence of real and composite deductions.

Let us derive the formula, which mutually connects the sequences of real and smallest composite deductions. Let us find for $h_k = k < N$ its smallest deduction from modulus/module M, for which we will use formula (7.5)

$$\dot{V}_k = x + iy = \frac{pr - qr'}{N} + \frac{pr' + qr}{N} i \qquad (7.43)$$

Page 421.

Here r and r' are the least non-negative residue of numbers pk and -qk on modulus/module N, i.e., r=pk-Nξ, $r' = -qk + N(\eta + 1)$, where $\xi =$ [pk/N] and $\eta = \left[\frac{qk}{N} \right]$ - integers part.

Substituting the value of r and r' in (7.43), we will obtain

$$\dot{V}_k = x + iy = \frac{p(pk - N\xi) - q[-qk + N(\eta - 1)]}{N} +$$
$$+ \frac{p[-qk + N(\eta + 1)] + q(pk - N\xi)}{N} i$$

it is final

$$\dot{V}_k = x + iy = [k - p\xi - q(\eta - 1)] + [p(\eta + 1) - q\xi] i. \quad (7.44)$$

where k=0, 1, 2, ..., N-1.

Example. Let $\dot{M} = 3 + 4i$, N=25. It is necessary for system $\dot{M}$ to find out the set of the represented numbers according to formula (7.44).

(1) Для $k = 0, 1, 2, 3, 4, 5, 6$. $\xi = 0$. $\eta = 0$.

$$\dot{V}_0 = -4 + 3i, \quad \dot{V}_1 = -3 + 3i, \quad \dot{V}_2 = -2 + 3i, \quad \dot{V}_3 = -1 + 3i.$$
$$\dot{V}_4 = 3i, \quad \dot{V}_5 = 1 + 3i, \quad \dot{V}_6 = 2 + 3i.$$

(2) Для $k = 7, 8$, $\xi = 0$, $\eta = 1$.

$$\dot{V}_7 = 1 + 6i, \quad \dot{V}_8 = 6i.$$

(3) Для $k = 9, 10, 11, 12$, $\xi = 1$, $\eta = 1$,

$$\dot{V}_9 = -2 + 10i, \quad \dot{V}_{10} = -1 + 10i, \quad \dot{V}_{11} = 10i; \quad \dot{V}_{12} = 1 + 10i.$$

(4) Для $k = 13, 14, 15, 16$, $\xi = 1$, $\eta = 2$.

$$\dot{V}_{13} = -2 + 13i, \quad \dot{V}_{14} = -1 + 13i, \quad \dot{V}_{15} = 13i, \quad \dot{V}_{16} = 1 + 13i.$$

(5) Для $k = 17, 18$ $\xi = 2$ $\eta = 2$

$$\dot{V}_{17} = -1 + 17i, \quad \dot{V}_{18} = 17i.$$

(6) Для $k = 19, 20, 21, 22, 23, 24$ $\xi = 2$ $\eta = 3$

$$\dot{V}_{19} = -3 + 20i, \quad \dot{V}_{20} = -2 + 20i, \quad \dot{V}_{21} = -1 + 20i, \quad \dot{V}_{22} = 20i.$$
$$\dot{V}_{23} = 1 + 20i, \quad \dot{V}_{24} = 2 + 20i.$$

Key: (1). For.

Let us further derive formula for the case of the least positive residues. Let for k<N be found out its least positive residue then according to formula (7.5) we will have

$$\dot{V}_k = x + iy = \frac{pr - qr'}{N} + \frac{pr' + qr}{N} i. \quad (7.45)$$

Page 422.

Here r and r' are the least positive residues of numbers pk and -qk on modulus/modula N; therefore

$$r = pk - N\left[\frac{\xi+1}{2}\right], \quad r' = -qk - N\left[\frac{\eta+1}{2}\right],$$
$$\xi = \left[\frac{2pk}{N}\right], \quad \eta = \left[\frac{2qk}{N}\right].$$

(7.46)

Let us rewrite (7.45), keeping in mind (7.46)

$$\dot{V}_k = \frac{p\left(pk - N\left[\frac{\xi-1}{2}\right]\right) - q\left(-qk - N\left[\frac{\eta+1}{2}\right]\right)}{N} +$$
$$+ \frac{p\left(-qk + N\left[\frac{\eta-1}{2}\right]\right) + q\left(pk - N\left[\frac{\xi-1}{2}\right]\right)}{N} i =$$
$$= \left(k - p\left[\frac{\xi-1}{2}\right] - q\left[\frac{\eta+1}{2}\right]\right) + \left(p\left[\frac{\eta+1}{2}\right] - q\left[\frac{\xi+1}{2}\right]\right) i.$$

Thus, the set of the represented numbers in this system $\dot{N}=p+qi$, where $(p, q)=1$, it is determined from the formula

$$\dot{V}_k = \left(k - p\left[\frac{\xi-1}{2}\right] - q\left[\frac{\eta+1}{2}\right]\right) +$$
$$+ \left(p\left[\frac{\eta-1}{2}\right] - q\left[\frac{\xi+1}{2}\right]\right) i.$$

(7.47)

Example. To find the set of the represented numbers in system $\dot{N}=3+4i$ of absolute-smallest deductions. Here N=25, therefore, giving k the sequence of values of 0, 1, 2, 3, ..., 24, we find through formula (7.47):

(1) для значений $k = 0, 1, 2, 3, \left[\frac{\xi+1}{2}\right]=0, \left[\frac{\eta+1}{2}\right]=0$
$$\dot{V}_0 = 0, \dot{V}_1 = 1, \dot{V}_2 = 2, \dot{V}_3 = 3;$$

(2) для $k = 4 \left[\frac{\xi+1}{2}\right]=0, \left[\frac{\eta+1}{2}\right]=1$
$$\dot{V}_4 = 3i;$$

(3) для $k = 5, 6, 7, 8, 9 \left[\frac{\xi+1}{2}\right]=\left[\frac{\eta+1}{2}\right]=1$
$$\dot{V}_5 = -2-i, \dot{V}_6 = -1-i, \dot{V}_7 = -i, \dot{V}_8 = 1-i, \dot{V}_9 = 2-i;$$

(4) для $k = 10, 11, 12 \left[\frac{\xi+1}{2}\right]=1, \left[\frac{\eta+1}{2}\right]=2,$
$$\dot{V}_{10} = -1+2i, \dot{V}_{11} = 2i, \dot{V}_{12} = 1+2i;$$

② для $k = 13, 14, 15$ $\left[\frac{\xi-1}{2}\right] = \left[\frac{\eta-1}{2}\right] = 2$,

$$\dot{V}_{13} = -1-2i, \quad \dot{V}_{14} = -2i, \quad \dot{V}_{15} = 1-2i;$$

② для $k = 16, 17, 18, 19, 20$ $\left[\frac{\xi+1}{2}\right] = 2$, $\left[\frac{\eta+1}{2}\right] = 3$,

$$\dot{V}_{16} = -2-i, \quad \dot{V}_{17} = -1-i, \quad \dot{V}_{18} = i, \quad \dot{V}_{19} = 1-i, \quad \dot{V}_{20} = 2-i;$$

② для $k = 21$ $\left[\frac{\xi+1}{2}\right] = \left[\frac{\eta+1}{2}\right] = 3$,

$$\dot{V}_{21} = -3i$$

② для $k = 22, 23, 24$ $\left[\frac{\xi-1}{2}\right] = 3$, $\left[\frac{\eta-1}{2}\right] = 4$,

$$\dot{V}_{22} = -3, \quad \dot{V}_{23} = -2, \quad \dot{V}_{24} = -1.$$

Key: (1). for the values. (2). for.

Page #23.

§7.9. Translation/conversion complex integers of the positional system into system M of real deductions and vice versa.

Let be given system $\dot{M} = \dot{m}_1 \dot{m}_2 \ldots \dot{m}_n = p - qi$ and $N_1, \dot{N}_2, \ldots, N_n, N$ and $\rho_1, \rho_2, \ldots, \rho_n, \rho$

respectively norm and the coefficients of the isomorphism of numbers $\dot{m}_1, \dot{m}_2, \ldots, \dot{m}_n, \dot{M}$.

Further, let for the representation in system M of real deductions is preset number $\dot{A}=a+bi$. Then according to the theorem of isomorphism we have $a+bi=h(\bmod \dot{M})$, where h is determined from condition $a+b\rho=h(\bmod N)$, however, since

$$\dot{M} = \dot{m}_1\dot{m}_2 \ldots \dot{m}_n \quad \text{и} \quad N = N_1 N_2 \ldots N_n,$$

that according to the property of comparisons we will obtain

$$a + bi \equiv h(\bmod \dot{m}_1);$$

and

$$a + bi \equiv h(\bmod \dot{m}_2); \ldots; a + bi \equiv h(\bmod \dot{m}_n)$$

$$a + b\rho \equiv h(\bmod N_1);$$

$$a + b\rho \equiv h(\bmod N_2); \ldots; a + b\rho \equiv h(\bmod N_n),$$

from $h \equiv h_j(\bmod N_j)$, it follows

$$a - b\rho \equiv h_1(\bmod N_1),$$
$$a - b\rho \equiv h_2(\bmod N_2).$$
$$\cdots \cdots \cdots \cdots \cdots$$
$$a - b\rho \equiv h_n(\bmod N_n).$$

and

$$a + bi \equiv h_1(\bmod \dot{m}_1), \qquad (7.48)$$
$$a - bi \equiv h_2(\bmod \dot{m}_2).$$
$$\cdots \cdots \cdots \cdots \cdots$$
$$a - bi \equiv h_n(\bmod \dot{m}_n).$$

hence

$$a - bi = (h_1, h_2, \ldots, h_n). \qquad (7.49)$$

Page 424.

Thus, for the determination of representation (7.49) is sufficient to find h_j from (7.48) with the help of the coefficient of the isomorphism ρ of $\dot{M}$. It is possible representation (7.49) to find, also, with the help of the coefficients of isomorphism $\rho_1, \rho_2, \ldots, \rho_n$. In fact, we have:

$$
\begin{aligned}
a + b\rho_1 &\equiv h_1 \,(\text{mod}\, N_1), \\
a + b\rho_2 &\equiv h_2 \,(\text{mod}\, N_2), \\
&\cdots\cdots\cdots\cdots \\
a + b\rho_n &\equiv h_n \,(\text{mod}\, N_n),
\end{aligned}
\qquad (7.50)
$$

whence we will obtain representation (7.49).

Theorem 7.13. If $\dot{M} = \dot{m}_1 \dot{m}_2 \ldots \dot{m}_n = (p_1 - q_1 i) \times (p_2 + q_2 i) \ldots (p_n - q_n i)$, $\rho_1, \rho_2, \ldots, \rho_n, \rho$

respectively the coefficients of isomorphism $\dot{m}_j$ and $\dot{M}$, then the coefficient of the isomorphism ρ of product $\dot{M}$ has a representation

$$
\rho = (\rho_1, \rho_2, \ldots, \rho_n) \qquad (7.51)
$$

in the system with bases/bases $N_1, N_2, \ldots, N_n$.

Proof. In order to avoid cumbersome calculations. The proof of theorem let us lead for n=2, i.e., for the case when

$$
\dot{M} = (p_1 + q_1 i)(p_2 + q_2 i) = (p_1 p_2 - q_1 q_2) + (q_1 p_2 - p_1 q_2) i = p - qi;
$$

from theorem condition we have

$$
\begin{aligned}
\mu_1 &= u_1 q_1 - v_1 p_1, \\
\mu_2 &= u_2 q_2 - v_2 p_2, \\
\rho &= u\,(q_1 p_2 - p_1 q_2) - v\,(p_1 p_2 - q_1 q_2),
\end{aligned}
$$

where u_1, u_2, v_1, v_2, u, v are connected with the conditions

$$
u_1 p_1 + v_1 q_1 = 1, \quad u_2 p_2 + v_2 q_2 = 1, \quad up + vq = 1. \quad (7.52)
$$

Page 425.

Let us find the smallest non-negative remainders/residues γ_1 and γ_2 number ρ from modulus/module $N_1=p^2{}_1+q^2{}_1$ and $N_2=p^2{}_2+q^2{}_2$. We have $\rho=k_1N_1+\gamma_1$ and $\rho=k_2N_2+\gamma_2$, whence $\gamma_1=\rho-k_1N_1$ and $\gamma_2=\rho-k_2N_2$ or after statement of expression ρ, N_1, N_2 we will obtain

$$\gamma_1 = u(q_1p_2 + p_1q_2) - v(p_1p_2 - q_1q_2) - k_1(p_1^2 - q_1^2),$$
$$\gamma_2 = u(q_1p_2 + p_1q_2) - v(p_1p_2 - q_1q_2) - k_2(p_2^2 + q_2^2). \tag{7.53}$$

Let us regroup right sides (7.53) relative to p_1, q_1 in the first and p_2, q_2 in the second equality

$$\gamma_1 = (p_2u + q_2v - k_1q_1)\,q_1 - (p_2v - q_2u + k_1p_1)\,p_1$$
$$\gamma_2 = (p_1u + q_1v - k_2q_2)\,q_2 - (p_1v - q_1u + k_2p_2)\,p_2.$$

Let us show that

$$u_1 = p_2u + q_2v - k_1q_1, \quad v_1 = p_2v - q_2u + k_1p_1,$$
$$u_2 = p_1u + q_1v - k_2q_2, \quad v_2 = p_1v - q_1u + k_2p_2$$

they satisfy with respect to first two conditions (7.52), for which we form

$$(p_2u + q_2v - k_1q_1)\,p_1 + (p_2v - q_2u + k_1p_1)\,q_1 =$$
$$= p_1p_2u + p_1q_2v - p_1k_1q_1 + p_2q_1v - q_1q_2u + p_1k_1q_1 =$$
$$= (p_1p_2 - q_1q_2)\,u + (p_1q_2 + p_2q_1)\,v.$$

Latter/last expression is equal to one according to third condition (7.52); therefore $\gamma_1=\rho_1$, analogously we will obtain

$$(p_1u + q_1v - k_2q_2)\,p_2 + (p_1v - q_1u + k_2p_2)\,q_2 =$$
$$= p_1p_2u + p_2q_1v - p_2q_2k_2 + p_1q_2v - q_1q_2u + p_2q_2k_2 =$$
$$= (p_1p_2 - q_1q_2)\,u + (p_1q_2 + p_2q_1)\,v,$$

which is also equal to unity according to latter/last condition (7.52); therefore $\gamma_2=\rho_2$. Consequently, ρ_1 and ρ_2 are the least

non-negative residue numbers ρ on modulus/module N_1, N_2, QED.

Page 426.

The validity of this theorem follows also directly from (7.48) and (7.50). In fact, since in comparisons (7.48) and (7.50) right sides are equal, then

$$a + b\rho \equiv a + b\rho_j \,(\mathrm{mod}\,N_j)$$

or

$$b(\rho - \rho_j) \equiv 0 \,(\mathrm{mod}\,N_j).$$

Since ρ and ρ_j do not depend on selection $\dot{A}=a+bi$ that let us assume that $(b, N_j)=1$, then $\rho - \rho_j \equiv 0 \,(\mathrm{mod}\,N_j)$, whence it follows that $\rho \equiv \rho_j(\mathrm{mod}\,N_j)$. i.e. $\rho = (\rho_1, \rho_2, \ldots, \rho_n)$.

Now according to the recently proved theorem, it is possible to indicate one more, moreover the most practical algorithm of the representation of the preset number a+bi in system $\dot{M}$. In fact, since $\rho = (\rho_1, \rho_2, \ldots, \rho_n)$, and $a = (\alpha_1; \alpha_2; \ldots \alpha_n)$ and $b = (\beta_1; \beta_2; \ldots \beta_n)$, then (7.48) it is possible to rewrite

$$\begin{aligned}
\alpha_1 + \beta_1\rho_1 &\equiv h_1 \,(\mathrm{mod}\,N_1), \\
\alpha_2 + \beta_2\rho_2 &\equiv h_2 \,(\mathrm{mod}\,N_2), \\
&\cdots\cdots\cdots \\
\alpha_n + \beta_n\rho_n &\equiv h_n \,(\mathrm{mod}\,N_n),
\end{aligned}$$

whence we consist that unknown deductions h_j are found from condition

$$\begin{aligned}
(\alpha_1, \alpha_2, \ldots, \alpha_n) &+ (\beta_1, \beta_2, \ldots, \beta_n)(\rho_1, \rho_2, \ldots, \rho_n) = \\
&= (h_1, h_2, \ldots, h_n).
\end{aligned}$$

Example. As the system let us take

$$\dot{M} = \dot{m}_1 \cdot \dot{m}_2 \cdot \dot{m}_3 \cdot \dot{m}_4 \cdot \dot{m}_5 \cdot \dot{m}_6 \cdot \dot{m}_7 \cdot \dot{m}_8 \cdot \dot{m}_9 \cdot \dot{m}_{10} =$$
$$= (1+i)(2+i)(3+2i)(4+i)(5+2i)(1+6i)(5+4i)(7+2i) \times$$
$$\times (6+5i)(3+8i) = 4\,749\,285 - 1\,291\,214i$$

here
$$N = N_1 \cdot N_2 \cdot N_3 \cdot N_4 \cdot N_5 \cdot N_6 \cdot N_7 \cdot N_8 \cdot N_9 \cdot N_{10} = 2 \cdot 5 \cdot 13 \cdot 17 \cdot 29 \cdot 37 \cdot 41 \times$$
$$\times 53 \cdot 61 \cdot 73$$

$$\rho = (\rho_1, \ \rho_2, \ \rho_3, \ \rho_4, \ \rho_5, \ \rho_6, \ \rho_7, \ \rho_8, \ \rho_9, \ \rho_{10}) =$$
$$= (1, \ 3, \ 5, \ 13, \ 12, \ 6, \ 9, \ 25, \ 11, \ 27).$$

Let us present number $\dot{A} = 3751 + 1842i$ in this system $\dot{M}$. For which let us find representations its component 3751 and 1842 in this system, i.a.

$$3751 = (L, 1, 7, 11, 10, 14, 20, 41, 30, 27)$$
$$1842 = (0, 2, 9, 6, 15, 29, 38, 40, 12, 17).$$

Page 427.

Then according to theorem 7.13 we find

$$3751 - 1842i = (1, 1, 7, 11, 10, 14, 20, 41, 30, 27) -$$
$$+ (0, 2, 9, 6, 15, 29, 38, 40, 12, 17) \cdot (1, 3, 5, 13, 12, 6, 9, 25, 11, 27) =$$
$$= (1, 1, 7, 11, 10, 14, 20, 41, 30, 27) + (0, 1, 6, 10, 6, 26, 14, 46, 10, 21) =$$
$$= (1, 2, 0, 4, 16, 11, 34, 5, 40, 48).$$

Let us now move on to the construction of the translation algorithms of numbers of the system $\dot{M}$ into the ordinary positional system. Is valid the following theorem.

Theorem 7.14. For system $\dot{M} = (p_1 + q_1 i)(p_2 + q_2 i) \dots (p_n + q_n i) = p + qi$ with norms $N_1, N_2, \dots, N_n, N$ and coefficients of isomorphism $\rho_1, \rho_2, \dots, \rho_n, \rho,$ as the orthogonal bases of system it is possible to take the least

positive residues of numbers $B_j = \frac{N}{N_j} \cdot k_j$ in moduli/modules $\dot{M}$, where $k_j < N_j$ are determined from condition

$$k_j \frac{N}{N_j} \equiv 1 \, (\text{mod} \, N_j).$$

Proof. Let in system $\dot{M}$ be is given the number

$$\dot{A} = a + bi = (\alpha_1 + \beta_1 i; \, \alpha_2 + \beta_2 i; \, \ldots; \, \alpha_n + \beta_n i),$$

then

$$\dot{A} \equiv (1, 0, 0, \ldots, 0)\,(\alpha_1 + \beta_1 i; \, 0, 0, \ldots, 0) + \ldots$$
$$\ldots + (0, 0, \ldots, 0, 1)\,(0, 0, \ldots, 0, \alpha_n + \beta_n i) \, (\text{mod} \, \dot{M}).$$

Here the numbers

$$\begin{aligned}
\dot{B}_1 &= (1, 0, 0, \ldots, 0), \\
\dot{B}_2 &= (0, 1, 0, \ldots, 0), \\
&\cdots\cdots\cdots\cdots \\
\dot{B}_n &= (0, 0, \ldots, 0, 1),
\end{aligned} \qquad (7.54)$$

as and in the real region, we will call the composite orthogonal bases of system $\dot{M}$.

If we the norm of bases N_j consider as the basis of system, then number $B_j = \frac{N}{N_j} \cdot k_j$, as is known, they are the orthogonal bases of this system; therefore

$$B_j \equiv 1 \, (\text{mod} \, N_j), \quad B_j \equiv 0 \, \left(\text{mod} \, \frac{N}{N_j}\right).$$

Page 428.

Let $\dot{B}_j = c_j + d_j i$ be the least positive residues of numbers B_j on modulus/module $\dot{M}$, i.e., $c_j + d_j i \equiv B_j \, (\text{mod} \, \dot{M})$, then, since $B_j < N$. on (7.14) $B_j \equiv c_j + d_j \rho \, (\text{mod} \, N)$, but by force $N = N_1 N_2 \ldots N_n$. and according to the

property of the comparisons

$$B_j \equiv c_j + d_j \rho \pmod{N_j}.$$

According to condition $B_j \equiv 1 \pmod{N_j}$, consequently, $c_j + d_j \rho \equiv 1 \pmod{N_j}$, whence on bases of theorem 7.2 we have $\dot{B}_j = c_j + d_j i \equiv 1 \pmod{\dot{m}_j}$.

Analogously we establish that

$$\dot{B}_j = c_j + d_j i \equiv 0 \left(\bmod \frac{\dot{M}}{\dot{m}_j} \right).$$

Thus, numbers $\dot{B}_j$ satisfy condition (7.54) of orthogonality, QED.

Theorem 7.15. Any complex integer $\hat{A} = (h_1, h_2, \ldots, h_n)$, represented in system $\dot{M}$, is the least positive residue of the number

$$h = B_1 h_1 + B_2 h_2 + \ldots + B_n h_n \pmod{N}$$

on modulus/module $\dot{M}$, where B_j — orthogonal bases of system.

Proof. Let representation $\dot{A}$ in system $\dot{M}$ in the real deductions take form $\dot{A} = a + bi = (h_1, h_2, \ldots, h_n)$. This means that $a + b\rho \equiv h_j \pmod{N_j}$ or $a + b\rho = (h_1, h_2, \ldots, h_n)$.

Consequently, if B_j — bases of system N, then

$$a + b\rho \equiv B_1 h_1 + B_2 h_2 + \ldots + B_n h_n \pmod{N} = h \pmod{N},$$

whence we obtain $\dot{A} = h \pmod{\dot{M}}$. Thus, absolutely the smallest deductions of numbers $\dot{A}$ and h on modulus/module $\dot{M}$ must be equal, that also proves theorem.

Let us consider the examples, which illustrate theorems 7.14 and 7.15. In these examples is accepted the system: $\dot{m}_1=1+1$, $\dot{m}_2=2+i$, $\dot{m}_3=3+2i$, $\dot{m}_4=4+i$, $M=41+23i$, $N_1=2$, $N_2=5$, $N_3=13$, $N_4=17$, $N=2210$, $\rho=(1,\ 3,\ 5,\ 13)$.

The orthogonal bases of system are equal to:

$$B_1 = 1105, \quad B_2 = 1326, \quad B_3 = 170, \quad B_4 = 1820.$$

Page 429.

Example. To determine the complex orthogonal bases of system. According to theorem 7.14 we have:

$$1105 \equiv c_1 + d_1 i \pmod{41 + 23i},$$
$$1326 \equiv c_2 + d_2 i \pmod{41 + 23i},$$
$$170 \equiv c_3 + d_3 i \pmod{41 - 23i},$$
$$1820 \equiv c_4 + d_4 i \pmod{41 - 23i}.$$

Further, after determining the least positive residues of numbers 1105, 1326, 170 and 1820 on the modulus/module $41+23i$, we will obtain the unknown bases:

$$\dot{B}_1 = 9 + 32i, \quad \dot{B}_2 = -21 - i, \quad \dot{B}_3 = 1 + 13i, \quad \dot{B}_4 = -11 - 3i.$$

Example. The complex number $\dot{A}$ has representation $\dot{A} = (1,\ 3,\ 6,\ 9)$. To convert it into the ordinary positional system.

According to theorem 7.15 let us find

$$h = 1105 \cdot 1 + 3 \cdot 1326 + 6 \cdot 170 + 9 \cdot 1820 \pmod{2210} = 383,$$

whence A=383 (modes 41+23i); therefore the least positive residue of number 383 on the modulus/module 41+23i gives the unknown complex number 4+3i.

DOC = 81023920   PAGE ● 714

REFERENCES.

1. Акушский И. Я. Многорегистровые схемы выполнения арифметических операций. «Вопросы теории математических машин». Физматгиз, 1958.

2. Акушский И. Я. Арифметические операции в системе остаточных классов. «Вопросы радиоэлектроники» серия VII, 1960 г., вып. 3.

3. Акушский И. Я., Хацкевич В. Х. Инверсные представления чисел в системе остаточных классов. «Цифровая вычислительная техника и программирование», вып. 2, 1967 г.

4. Акушский И. Я., Юдицкий Д. И. Некоторые вопросы логики и структуры УЦВМ высокой производительности. «Вопросы радиоэлектроники», серия VII, 1960 г., вып. 3.

5. Акушский И. Я., Юдицкий Д. И., Позиционные характеристики числовых представлений в остаточных классах. «Цифровая вычислительная техника и программирование», вып. 2, 1967 г.

6. Акушский И. Я. Машинная арифметика в системе остаточных классов. Доклад на IV Всесоюзном математическом съезде. Ленинград, 1961 г., труды съезда, т. IV.

7. Анисимов Б. В., Четвериков В. Н. Основы теории и проектирования цифровых вычислительных машин. Машгиз, 1962.

8. Виноградов И. М. Основы теории чисел. Изд-во «Наука», 1965.

9. Богданов А. В. Выбор режима элементов, управляющих диодной матрицей в ВМ большого быстродействия. «Электронная техника». серия VI, 1966 г., № 2.

10. Гаусс К. Ф. Труды по теории чисел. Изд-во АН СССР, 1959.

11. Геллер С. И., Долгов А. И., Золин В. В. Алгоритмы основных операций в системе счисления остаточных классов и их реализации. В сборнике «Вопросы построения быстродействующих ЦВМ», АРТА. Харьков, 1965.

12. Глушков В. М. Синтез цифровых автоматов. Физматгиз, 1962.

13. Дроздов Е. А., Пятибратов А. П. Автоматическое преобразование и кодирование информации. Изд-во «Советское радио», 1964.

14. Дэвенпорт Г. Высшая арифметика. Изд-во «Наука», 1965.

15. Жуков-Емельянов О. Д. Некоторые вопросы, связанные с умножением и делением в системе остаточных классов. ИТМ и ВТ. Электронные вычислительные машины, 1964.

Page 431.

16. Жуков-Емельянов О. Д. Цепной алгоритм в системе остаточных классов. ИТМ и ВТ. Электронные вычислительные машины, 1965.

17. Зарепин Ю. Г. Корректирующие коды для передачи и переработки информации. Изд-во «Техника», Киев, 1965.

18. Иокки Д. Кодирование методом вычетов и применение его в космической связи. «Зарубежная радиоэлектроника», 1963 № 9.

19. Карцев М. А. Арифметические устройства электронных цифровых машин. Физматгиз, 1958.

20. Келдыш Л. В., Ляпунов А. А., Шура-Бура М. Р. Математические вопросы теории счетных машин. «Вестник АН СССР», 1956, № 11.

21. Китов А. И., Криницкий Н. А. Электронные цифровые машины и программирование. Физматгиз, 1961.

22. Кобринский Н. Е. Математические машины непрерывного действия. ГИТТЛ, 1954.

23. Кобринский Н. Е., Трахтенброт Б. А. Введение в теорию конечных автоматов. Физматгиз, 1962.

24. «Коды с обнаружением и исправлением ошибок». Пер. с англ., под ред. А. М. Петровского. Изд-во иностранной литературы, 1956.

25. Корн Г., Корн Т. Электронные моделирующие устройства. Изд-во иностранной литературы, 1955.

26. Мирончиков Е. Т., Колесник В. Д. Об арифметических корректирующих кодах. «Радиотехника и электроника», 1963, № 1.

27. Моисил Г. Алгебраическая теория дискретных автоматических устройств. Изд-во иностранной литературы, 1963.

28. Паперков А. А. Логические основы цифровых машин и программирования. Изд-во «Наука», 1965.

29. «Передача цифровой информации». Изд-во иностранной литературы, 1963.

20. Питерсон У. У. Коды, исправляющие ошибки. Изд-во «Мир», 1964.

31. Радченко А. Н., Мирончиков Е. Т. Многотактные методы исправления одиночных и многократных близко расположенных ошибок в групповых кодах. «Радиотехника и электроника», 1961, № 11.

32. Реферат о УВМ «Эпос». Реферативный журнал «Автоматика, телемеханика и вычислительная техника», 1964, № 2.

33. Ричардс Р. К. Арифметические операции на цифровых вычислительных машинах. Изд-во иностранной литературы, 1957.

34. Ричардс Р. К. Элементы и схемы цифровых вычислительных машин. Изд-во иностранной литературы, 1961.

35. Сифоров В. И. О помехоустойчивости систем с корректирующими кодами. «Радиотехника и электроника», 1961, № 11.

36. Реферат «Сравнение чисел и определение переполнения в ЦВМ, использующих модульную арифметику». Реферативный журнал «Кибернетика», 1964.

37. «Теория кодирования». Пер. с англ., под ред. Э. Л. Блоха. Изд-во «Мир», 1964.

Page 432.

38. «Теория передачи сообщений». Пер. с англ. Изд-во иностранной литературы, 1957.

39. Тейтельбаум В. Н. Сравнение чисел в чешской системе счисления. «Доклады АН СССР, 1958, т. 121, № 5.

40. Удалов А. П., Супрун Б. А. Избыточное кодирование при передаче информации двоичными кодами. Изд-во «Связь», 1964.

41. Файн С. Б. Некоторые вопросы машинной арифметики системы остаточных клапанов. Труды ВЦ АН Груз. ССР, 1964.

43. Фано Р. М. Передача информации статистическая теория связи. Изд-во «Мир», 1965.

44. Фельдман Б. Я. К вопросу о минимальном базисе для системы остаточных классов. «Вопросы радиоэлектроники», 1963, сер. VII, вып. I.

45. Фельдбаум А. А. Вычислительные устройства в автоматических системах. Физматгиз, 1959.

46. Харкевич А. А. Борьба с помехами. Физматгиз, 1963.

47. Харкевич А. А. Одна теорема, относящаяся к корректирующим кодам. «Радиотехника», 1962, № 5.

48. Чебышев П. Л. Полное собрание сочинений, т. 1. Изд-во АН СССР, 1946.

49. Шеннон К. Э. Работы по теории информации и кибернетике. Изд-во иностранной литературы, 1963.

50. Юдицкий Д. И. Вопросы синтеза устройства управления УЦВМ. «Вопросы теории математических машин». Вып. 2, Физматгиз, 1962.

51. Юдицкий Д. И. О путях реализации системы остаточных классов. «Вопросы радиоэлектроники», серия VII, 1960 г., вып. 3.

52. Beadles R. L. The complementation of a modular arithmetic computer with binary logic elements. Proc. 7-th Nat. Convent, Military Electronics, Washington, 1963.

53. Cheney P. W. A digital correlator based on the residue number system. IRE Trans. on El. comp., 1961, EC-10, № 1.

54. Garner H. The residue number system. IRE Trans. on EL. Comp., 1959, v. 8, June.

55. Gaffin R. M. A special purpose computer for solving linear simultaneous equations using the residue number system. IRE Trans. Electronic comput., 1962, 11, N 2.

56. Keir Y. A., Cheney R. W., Tannenbaum M. Division and overflow detection in residue number system. IRE Trans. on El. comp., 1962, v. 11, № 4.

57. Knittee I., Zeller K. Berechungen ohne Abrundung mit der kongruenten Methode. Z. angew. Math. und Mech., 1960, v. 40.

58. Lean M., Aspinall D. A decimal adder using a stored addition table. PIEE. v. 105, pt. B, № 20, 1958, March.

59. Levine M. R., Levy E., Baker A. M. Modular arithmetic on ultra high-speed computation technique for aiborne digital computers Ballist Missile and Aerospace Technol., v. 2. Ballist Missile and space electronics, 1961.

60. Merrill R. D. Improving digital computer performance using residue number theory. IEEE Trans. EL. comp., 1964, v. 13, № 2.

Page 433.

61. M e t r o p o l i s N., A s h e n h u r s t R. L. Significant digit computer arithmetic. IRE Trans. on EL. comp., 1958, v. 7, № 4.

62. N a d l e r M. A high speed electronic arithmetic unit for automatic computing machines. Acta techn. (ceskasl), 1956, v. 1, № 6.

63. N o t h m a n M. H. Combined analog-digital control systems. Electr. Manufact., 1958, № 6.

64. P a u l P. Y. Some factors affecting the accuracy of electronic analogue computers. Actes. Jouries internat. analog., 1955

65. P e t e r s o n W. W. On checking an adder. IBM Journal of research and development, 1958, v. 2, № 2.

66. R o n a l d M. G. A computer for solving linear simultaneous equations using the residue number system. IRE Trans. on EL comp, 1961, EC-10, № 1.

67. S v o b o d a A., Valach M. Operatorve obvody. Stroje na zpacováni informaci, sbornik III, Nak 1, CSAV, 1955.

68. S v o b o d a A. Rational numerical system of residual classes. Stroje na zpacováni informaci, sbornik V, Nak 1, CSAV, 1957.

69. S v o b o d a A. The numerical system of residue classes in mathematical machines. Inform. processing, 1960.

70. S v o b o d a A. Le systéme numerique de classes residuelles dans les machines mathematiques. Automatisme, 1960, t. V, № 1—2.

71. S v o b o d a A. The numerical system of residue classes in mathematical machines. Informat. processing, Paris—München—London, 1960.

72. S v o b o d a A. Decimal arithmetic unit. Stroje na zpracov. inform. 8, 1962.

73. S z a b o N. Sign detection in nonredundant residue systems. IRE Trans. on El. comp., 1962, v. 11, № 4.

74. S z a b ó N. Recent advances in modular arithmetic. Switch theory Space Technol. Stanford, Calif. Univ. Press., 1963.

75. T a n a k a R. I. Some options in the design of a residue arithmetic computer. Proc. Nat. El. Conf. Chicago III, 1963.

76. V a l a c h M. Vznik kodu a ciselne zbytkovych trid. Stroje na zpracovani informaci, sbornik III, Nak I CSAV, 1955.

77. V a l a c h M. Abbilding der Zahen und der Arithmetishen Operationen im Restklassen System. Ber. Internat. Math. Kollag. Non. 57, 1955.

78. V a l a c h M. Prevod cisel ze so-ustavy zbytkových trid do polydické soustavy zmenou metrika periody. Stroje zprocav. inform., 1956, № 4.

79. Z w e i z i g L. K. Data encoder for general instrumentation. Teletech. 1955, v. 14, № 3.

Pages 434-439.

No typing.